



Financial
Intelligence Unit



Annual Report 2020

Financial Intelligence Unit

Annual Report 2020

Financial Intelligence Unit

Table of Contents

Preface	7
Overview of the FIU	9
Suspicious Transaction Reports	13
Total Number of Suspicious Transaction Reports for Reporting Year 2020	15
Total Number of Suspicious Transaction Reports, Categorised By Subgroups of Reporting Entities	16
Assessment Results for Suspicious Transaction Reports in 2020	22
Feedback Reports from Public Prosecution Authorities	24
Temporary Freezing Orders	28
Proliferation Financing	31
Transactions	32
Typologies and Trends	35
Description and Continuation of Key Risk Areas	36
Special Topic Covid-19	39
Key Risk Area Trade-Based Money Laundering	53
Key Risk Area Commercial Fraud	57
Key Risk Area Use of New Payment Methods	63
Key Risk Area Misuse of NGOs/NPOs	71
National Cooperation	77
Cooperation with Law Enforcement Agencies	79
Cooperation with Supervisory Authorities	81
Requests from Domestic Authorities	82
Cooperation with the Reporting Entities under AMLA	86
International Cooperation	91
Information Exchange with other FIUs	92
International Committee Work	101

List of Figures	106
List of Tables	107
List of Abbreviations	108

Dear Readers,

the prevention of and fight against money laundering and terrorist financing faced new challenges in the reporting year 2020. The Covid-19 pandemic and its consequences have had a deep and lasting impact on all areas of life. The activities of the Financial Intelligence Unit (FIU) were also affected in many ways by the consequences of the virus outbreak.

The risk-based approach of the FIU, which was already introduced in 2019 and further intensified in 2020, proved to be particularly effective in a fast-moving, divergent environment. Through the continuous review and event-driven adjustment of work and key risk areas, the FIU was able to react promptly to changing crime patterns and, for example, to forward target-oriented suspicious transaction reports (STRs) related to Covid-19 emergency aid fraud to the relevant law enforcement agencies. In chapter 'Typologies and Trends', you can learn more about the insights gained through these STRs and the increased reporting volume under Covid-19.

In this challenging year, new ways of communication were established to continue the important national and international collaborations and to strengthen ongoing cooperations. Therefore, I would like to sincerely thank all national and international partners.

Compared to the previous year, the number of reports in 2020 increased by another 25%, with a significant growth even without considering the reports related to the Covid-19 pandemic. The trend of the previous years thus continues and endorses the FIU in the consistent performance of its filter function as well as the implementation of the risk-oriented working method. More information on the adaptation and further development of the risk-based approach can be found in the section 'Overview of the FIU'.



Since the beginning of 2020, the FIU has been in the midst of intensive preparations for the fourth audit by the Financial Action Task Force (FATF). For this purpose, a working group was established within the customs administration at the beginning of 2019, to which since then specific measures have been assigned to in order to prepare for the audit. The audit is expected to be completed in 2021.

With regard to the considerable staff increase, particularly due to the increase in statutory tasks, the FIU is conducting a profound process-oriented analysis of its assignments that is supported by an external consulting company. The aim is to ensure that the organisational structure of the FIU is adapted to the changed conditions, in addition to the demands of process organisation and the associated process optimisation. This has already been partially implemented at the time of publication of this report; in particular, the FIU has now been set up as a separate directorate within the Central Customs Authority (GZD). Other required framework conditions are to be determined and quickly implemented in the course of 2021.

With this consistent further development, we as the FIU Germany, together with our partners, will continue to resolutely prevent and combat money laundering and terrorist financing in the future and will also be able to master new challenges.

Christof Schulte
Head of the FIU

Overview of the FIU

Overview of the FIU

The FIU is the national central office for financial transaction investigations. Under the umbrella of the Central Customs Authority (GZD), it is an independent and administratively oriented authority responsible for receiving, collecting and analysing suspicious transaction reports (STRs) in accordance with the Anti-Money Laundering Act (AMLA).

According to international regulations, all states are obliged to set up so-called central offices (Financial Intelligence Units – FIUs). In the Federal Republic of Germany, the FIU fulfils its legal mandate and is thus responsible in particular for the central receipt of STRs submitted by those parties obliged under the AMLA. Unusual or suspicious financial transactions contained in these reports, which could be related to money laundering or terrorist financing, are processed appropriately with varying depths of analysis. Since its reorganisation, the FIU has pursued a multidisciplinary approach and deployment of personnel in order to be able to assess a STR from the most diverse perspectives with the corresponding expertise. As a central hub, the FIU brings together relevant information and data from other authorities and agencies so that a comprehensive assessment can take place regarding suspicions of money laundering or terrorist financing. Only those reports that are deemed to be of value in the operational

individual case analysis are then forwarded to law enforcement agencies and other competent bodies. Through national forms of cooperation and collaboration with the supervisory authorities as well as the through progressive international networking with other FIUs, the FIU contributes to bundling competences worldwide and creating important synergy effects.

In addition to the operational analysis of STRs, the FIU can identify new methods and trends in the area of money laundering and terrorist financing through strategic analysis independent of individual cases. The findings are processed accordingly and made available both to the operational analysis units as an information module and to the reporting entities as well as partner authorities in the form of white and typology papers. In terms of preventive actions raising awareness and exchanging information with obligated parties is another important task of the FIU.

Adaptation and Further Development of Risk-oriented Working Methods

In order to interlock with the National Risk Assessment (NRA)¹ and in addition identify new methods and phenomena in the area of money laundering and terrorist financing, the FIU has already adopted a more risk-based approach in 2019 in accordance with international requirements.² Following the positive experience of the previous

year, the FIU consistently pursued and developed its risk-based approach in the reporting year 2020. Accordingly, since the beginning of the year, every incoming information – and thus in particular STRs pursuant to Sections 43, 44 AMLA – has been handled following the principles of the risk-based approach (RBA). STRs are continuously evaluated

1 The final report of the NRA was published in October 2019 (available on the website of the Federal Ministry of Finance, see https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.html).

2 See also the Annual Report 2019 (available on the website of the FIU at https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html).

on a risk basis to determine which information requires further processing in accordance with the FIU's legal core mandate. Only those STRs for which the FIU has identified a need for further analysis on the basis of the RBA are then transferred for in-depth analysis.

By using the corresponding filtering methods, the incoming STRs are prioritised. In this way, it is primarily STRs that can be assigned to a work

priority or key risk area of the FIU that reach the immediate further in-depth analysis. This does not affect the processing of cases with a possible connection to terrorist financing, which, as a key risk area, are always subjected to an in-depth analysis. STRs pursuant to Section 46 (1) AMLA³ are also always processed immediately. Since autumn 2020, the filtering of STRs has also been supported by 'FIU Analytics', an IT component based on artificial intelligence.

Further Development of the Statistics Concept

Pursuant to Section 28 (1) sentence 2 no. 10 AMLA, the FIU keeps the statistics required by the current EU Money Laundering Directive, which are published in particular in the annual report. In addition to the legal requirements for the collection of statistics, requirements also arise from internal process management and international cooperation. For this purpose, the FIU is continuously

improving its statistical system. With further adjustments for the consistent implementation of the RBA at the turn of the year 2019/2020 and the associated reorganisation of processes, the opportunity was taken to refine the statistics system across all units. Now it is possible to obtain more detailed statistical information and to better map internal processes with the existing IT procedure.

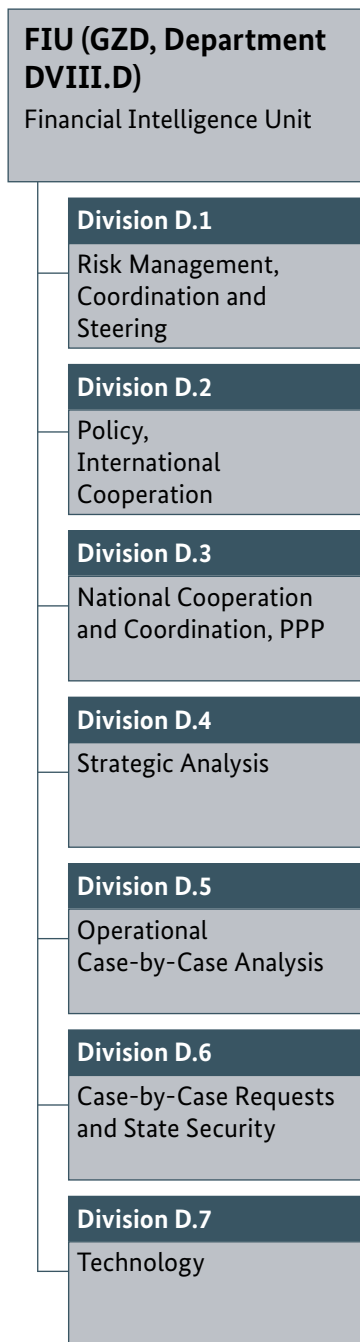
Further Development of the FIU – Implementation of the New Organisational Structure

In order to perform its duties, the FIU was set up as an administrative authority with operational independence. In the course of the FIU's continuing personnel expansion, the restructuring decided in 2019 was implemented organisationally as of July 2020. Since then, the FIU has been divided into a total of seven divisions, which are subdivided into different departments and units. The FIU's staffing needs to continue in order to increase significantly due to new legal tasks and the steadily rising volume of STRs. In this context, and

especially against the back-ground of further optimisation of its organisational processes, the FIU was developed into a separate directorate within the Central Customs Authority (GZD) as of 1 May 2021.

Further specialist information and current news can be found on the FIU's web page at www.fiu.bund.de.

³ Suspicious Transaction Reports (STRs) pursuant to Section 46 (1) AMLA are so-called urgent cases. The transaction on which the report is based may only be carried out after consent has been given or after three working days have elapsed. The reporting entity is thus subject to a temporary standstill obligation. The FIU assesses the facts immediately and, as a rule, conclusively processes them no later than one working day after receipt of the corresponding STR.



Organisational Structure in the Reporting Year

The main tasks of **Division D.1** are to initiate and accompany the process-oriented further development of the FIU’s fulfilment of its duties. Among other things, parliamentary and press queries are coordinated here.

Division D.2 bundles the following tasks: policy (including legal issues, business standards and development, FIU-specific organisational development and controlling) and international cooperation.

Division D.3’s mission is to ensure cooperation and exchange with the national law enforcement agencies and supervisory authorities and with the reporting entities under the German Anti-Money Laundering Act. This also comprises cooperation within the scope of public-private partnerships (PPP).⁴

The Strategic Analysis department within **Division D.4** executes non case-specific evaluations and analyses. Findings on typologies and trends are forwarded to other areas of the FIU, the authorities and reporting entities, dependent on the situation.

Case-by-case analysis within the remit of combating money laundering is executed in **Division D.5**. Here, STRs are subject to an initial risk-based assessment, analysed and disseminated to the relevant authorities as necessary.

Division D.6 analyses STRs related to terrorist financing or matters of state security and is the central contact point for all national and international partners in the field of operational cooperation (Money Laundering and Counter Terrorist Financing).

Division D.7 is charged, inter alia, with centralised specialist supervision of the FIU-specific specialised IT software solution goAML and coordinating the further development of the IT landscape for the FIU.

⁴ For more information on PPP, see the section on ‘National Cooperation’.

Suspicious Transaction Reports

Total Number of Suspicious Transaction Reports for Reporting Year 2020

Total Number of Suspicious Transaction Reports, categorise by Subgroups of Reporting Entities

Assessment Results for Suspicious Transaction Reports in 2020

Feedback Reports from Public Prosecution Authorities

Temporary Freezing Orders

Proliferation Financing

Transactions

Suspicious Transaction Reports

As central office, the FIU receives and analyses all STRs and information on suspicious financial transactions that could be related to money laundering or terrorist financing. The following overview will take a detailed look at the STRs received. This concerns reports submitted by reporting entities, financial and supervisory authorities that were received by the FIU in 2020⁵. In the following information that was reported to the FIU pursuant to Section 30 (1) No. 3-4 AMLA is not counted as STRs from reporting entities.

The electronically received STRs are subjected to operational analysis in several work steps while applying consistently the risk-based approach.

Receipt of report – Analysis – Decision

After receipt of the STR the report runs through an automated basic search in the course of which the data contained in the report are matched with other data bases in order to collate the findings in a targeted manner.

Using the RBA, the STR is continuously assessed to determine which information should be subjected to further analysis. In the course of the initial assessment, the reports are also prioritised. Suspicious transaction reports (STRs) that can be assigned to a work or key risk area⁶ of the FIU, represent a matter pursuant to Section 46 (1) AMLA or contain possible references to terrorist financing and state security are immediately transferred to the in-depth analysis. Otherwise, the STRs remain in the monitoring phase for the time being. Afterwards, they are continuously collated

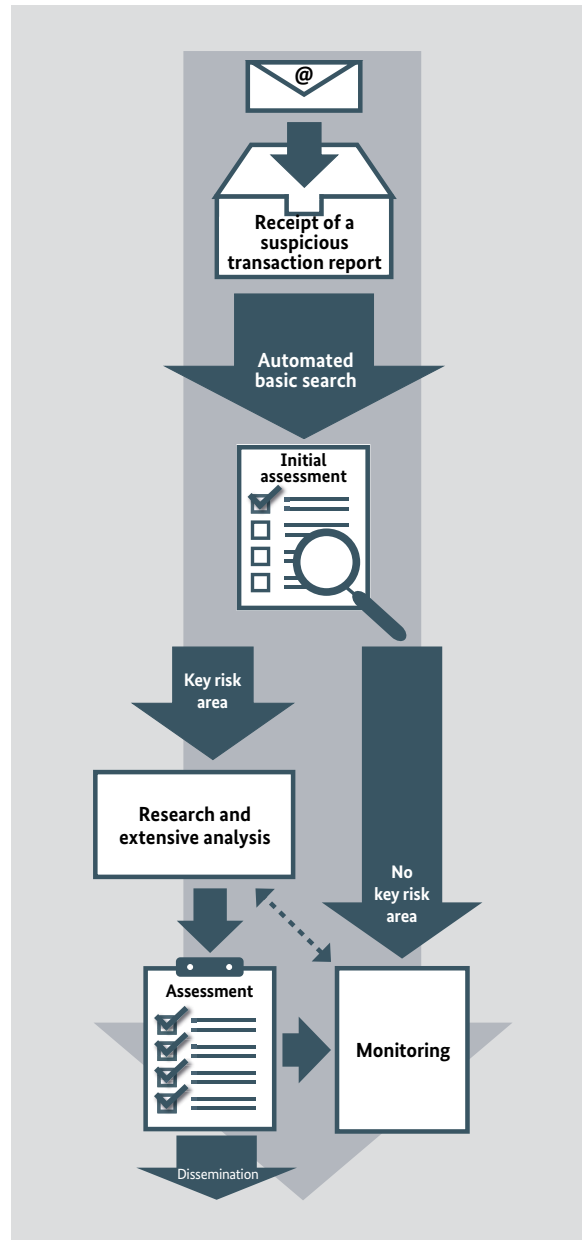


Figure 1: Process Sequence for Operational Analysis

with the present data and, if necessary, merged with further information at a later point in time and transferred to a detailed analysis.

⁵ Reports that have been submitted in accordance with Sections 43 and 44 of the German Anti-Money Laundering Act (AMLA) and Section 31 b of the German Tax Code (AO) are considered here. Thus, all reports and notifications that fall under Section 30 (1) No. 1-2 AMLA are listed.

⁶ For a list of the key risk areas, see the section ‘Typologies and Trends’.

If, in the course of a deeper analysis it is established that assets have a link to money laundering, terrorist financing or other criminal acts,

a dissemination in form of an analysis report is sent to the responsible Law Enforcement Agencies (LEA) and other competent authorities.

Total Number of Suspicious Transaction Reports for Reporting Year 2020

The FIU received a total of 144,005 STRs in 2020. Compared to the 114,914 STRs received in 2019 this is an increase of about 25%. With an absolute increase of about 29,000 reports, this represents the second highest increase in STRs within one year. Within the last ten years, the annual number of reports has increased by more than twelve times.

Thus, the trend of an increasing number of reports continues. A large part of these reports are STRs related to Covid-19 and the associated new mod operandi of money laundering. But even without the reports related to the Covid-19 pandemic, there has been an increase in the number of reports.⁷

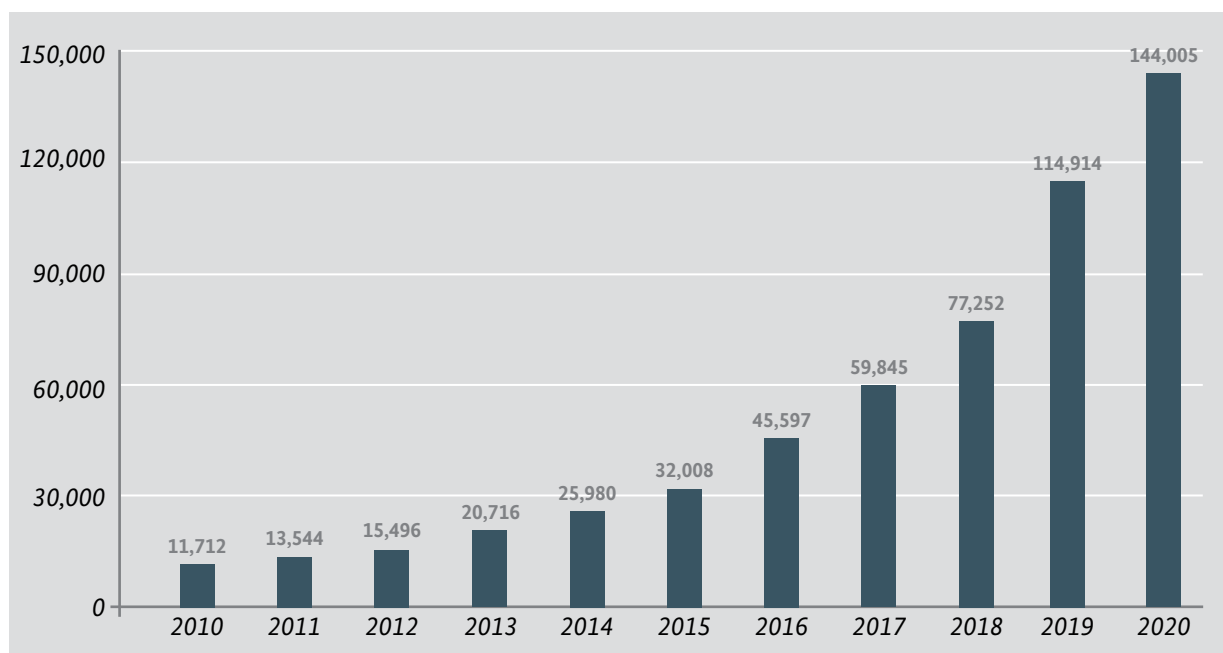


Figure 2: Development of the Number of Suspicious Transaction Reports According to the AMLA (2010 – 2020)

⁷ For more information on the Suspicious Transaction Reports (STR) related to the Covid-19 pandemic, see 'Special Topic Covid-19' in the section 'Typologies and Trends'.

The continuing increase in the number of incoming STRs encourages the FIU to consistently apply its filter function and to pass on matters of value to the competent authorities in a targeted manner. The risk-based approach that was introduced in 2019 was further strengthened. This enables a targeted steering of resources to the most important areas in the prevention and combating of money laundering and countering terrorist financing in terms of a common understanding of risk among all actors involved.

In the reporting year, a total of almost 3,600 STRs that had a potential connection to terrorist financing and other crimes relevant to the state security were received. In relation to the total volume of all STRs received, the share of these STRs is about 2%.⁸

Within the framework of an in-depth evaluation, these approximately 3,600 reports were first examined for relevance to state security or indications of links to terrorist financing. In the case of a positive check, the report was analysed in depth.

Total Number of Suspicious Transaction Reports, Categorised by Subgroups of Reporting Entities

In this reporting year as well as in the year before, the increase in the number of reports extends to both the financial and the non-financial sector. Only the number of reports from authorities and other reporting entities declined slightly compared to the previous year. The majority of reports, around 97%, continue to originate from the financial sector. With an increase of more than 27,000 reports, the increase in this sector amounts to almost 25%. After the decline in the previous year, a disproportionate increase of almost 33%

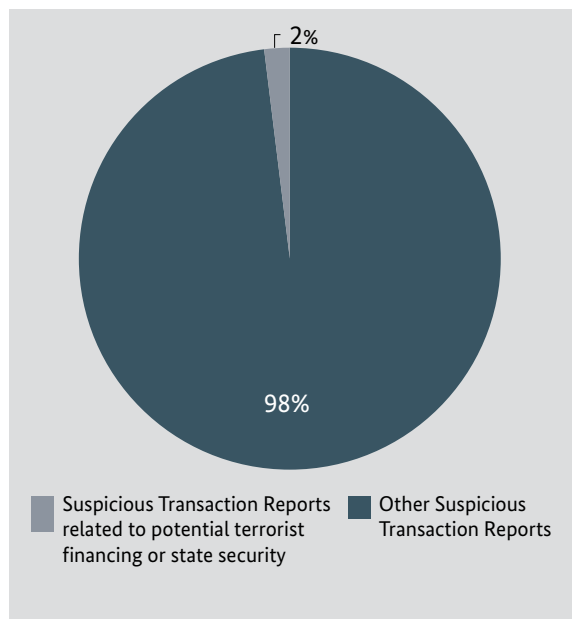


Figure 3: Relative Proportion of Suspicious Transaction Reports Related to Potential Terrorist Financing or State Security

Particularly noteworthy in this context are the key risk areas ‘Misuse of NGOs/NPOs’ and ‘Misuse of Money and Value Transfer Services’.⁹

was recorded in the number of STRs from financial services institutions. These are now close to the level of 2018 again. In the financial sector, only reports from payment institutions and electronic-money institutions as well as from asset management companies decreased in 2020.

While the total reporting volume increased by about 25%, there was again a disproportionate increase of almost 90% in the non-financial sector compared to 2019. In the previous year, the rise

⁸ A comparison with the figures reported in the annual reports of previous years is not possible due to internal (technical) changes in the generation of data by the FIU. Due to the consistent implementation of the risk-based approach and the associated prioritisation, only relevant STRs are forwarded for in-depth analysis in the area responsible for terrorist financing and state security. If a connection to terrorist financing or state security can already be ruled out during the initial screening, the report is not included in the number of STRs with a potential connection to terrorist financing or state security.

⁹ See the section ‘Typologies and Trends’.

was mainly caused by the reporting volume of organisers and brokers of games of chance, whereas the increase in this reporting year is due to the subgroups of reporting entities of notaries. There is a clear connection with the entry into force of the Ordinance on reporting requirements in the Real Estate Sector under the Anti-Money Laundering Act (GwGMeldV-Immobilien) on 1 October

2020.¹⁰ The FIU also received significantly more STRs from financial companies and estate agents. In contrast, there was a sharp decline in reports from the games of chance sector and traders in goods, which might be explained by the pandemic-related closures. Overall, the share of reports from the non-financial sector rose from a good 1.3% in the previous year to just under 2%.

	Reporting entities	2018	2019	2020	Change 2019/2020
Financial sector	Credit institutions	65,132	103,697	129,108	↗
	Financial service institutions	10,552	7,528	9,983	↗
	Payment institutions and electronic money institutions	264	290	238	↘
	Agents	35	650	730	↗
	Independent business persons	0	0	0	→
	Insurance undertakings	137	232	233	↗
	Asset management companies	17	42	33	↘
	Total of Suspicious Transaction Reports from the financial sector	76,137	112,439	140,325	↗
Non-financial sector	Financial companies	7	39	338	↗
	Insurance intermediaries	4	17	6	↘
	Lawyers	22	21	23	↗
	Legal advisors who are members of a bar association	0	0	0	→
	Patent attorneys	0	0	0	→
	Notaries	8	17	1,629	↗
	Legal advisors	0	3	0	↘
	Auditors and chartered accountants	2	0	7	↗
	Tax advisors and authorised tax agents	4	8	15	↗
	Trustees, service providers for trust companies	1	15	13	↘
	Estate agents	31	84	135	↗
	Organisers and brokers of games of chance	150	754	252	↘
	Traders in goods	368	554	436	↘
	Total of Suspicious Transaction Reports from the non-financial sector	597	1,512	2,854	↗
Other	Supervisory authority	54	149	144	↘
	Fiscal authorities	414	697	608	↘
	Other Suspicious Transaction Reports	50	117	74	↘
	Total	77,252	114,914	144,005	↗

Table 1: Number of Suspicious Transaction Reports According to Subgroups of Reporting Entities

¹⁰ For an explanation of the AMLA Real Estate (GwGMeldV-Immobilien), see the comments on 'Registered and Active Reporting Parties' later in this section.

Registered and Active Reporting Entities

As part of the amendment to the Anti-Money Laundering Act on 1 January 2020, Section 45 (1) sentence 2 AMLA was amended to the effect that reporting entities must register electronically with the FIU irrespective of the submission of a STR. This obligation will come into effect when the new information network of the FIU goes into operation – which has not yet happened – but no later than 1 January 2024.

Since this change in the law, there has been a significant increase in registrations. While there were only around 2,000 new registrations in 2019, around 7,700 additional reporting entities registered in 2020. In 2017, the year the electronic reporting system for STRs of money laundering went live for the first time, there were around 2,000 registrations, and in 2018 over 1,100 reporting entities were registered.

The total number of registered reporting entities as of 31 December 2020 was approximately 12,600 (excluding authorities and foreign FIUs¹¹).

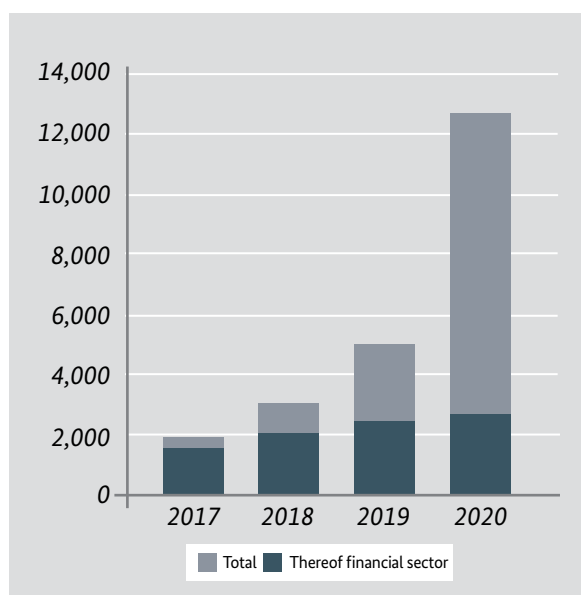


Figure 4: Increase of Reporting Entities Registered with the FIU

The increase in registrations is not equally divided among all subgroups of reporting entities. This can be explained, among other things, by the fact that chambers of the legal professions and individual associations in the non-financial sector in particular have sensitised their members to register with the FIU promptly as a precaution when the amendment to the law came into force.

With the entry into force of the Ordinance on reporting requirements in the Real Estate Sector under the Anti-Money Laundering Act (**GwGMeldV-Immobilien**) on 1 October 2020, there was a significant increase in registrations for the electronic reporting portal goAML, especially from all reporting entities of lawyers and notaries. In order to further improve the registration process in line with the reporting behaviour and to increase the registration quality, intensive co-ordination discussions took place with the Federal Chamber of Notaries. The results achieved jointly were then made available to the regional chambers of notaries by the Federal Chamber of Notaries in order to reach the largest possible number of reporting entities from this group.

Ordinance on Reporting Requirements in the Real Estate Sector under the Anti-Money Laundering Act (**GwGMeldV-Immobilien**)

The Ordinance on reporting requirements in the Real Estate Sector under the Anti-Money Laundering Act (**GwGMeldV-Immobilien**) specifies the reporting obligations of certain professionals – in particular lawyers, notaries, auditors and tax advisors in connection with real estate transactions. These professionals are required to report to the FIU certain typified circumstances that indicate a possible link to money laundering.

11 Reporting entities that registered with the FIU in the past but have since informed the FIU that they no longer exist (e.g. due to business closure or change of name) are also not included.

The following figure shows the development of new registrations of selected subgroups of

reporting entities over the last few years.

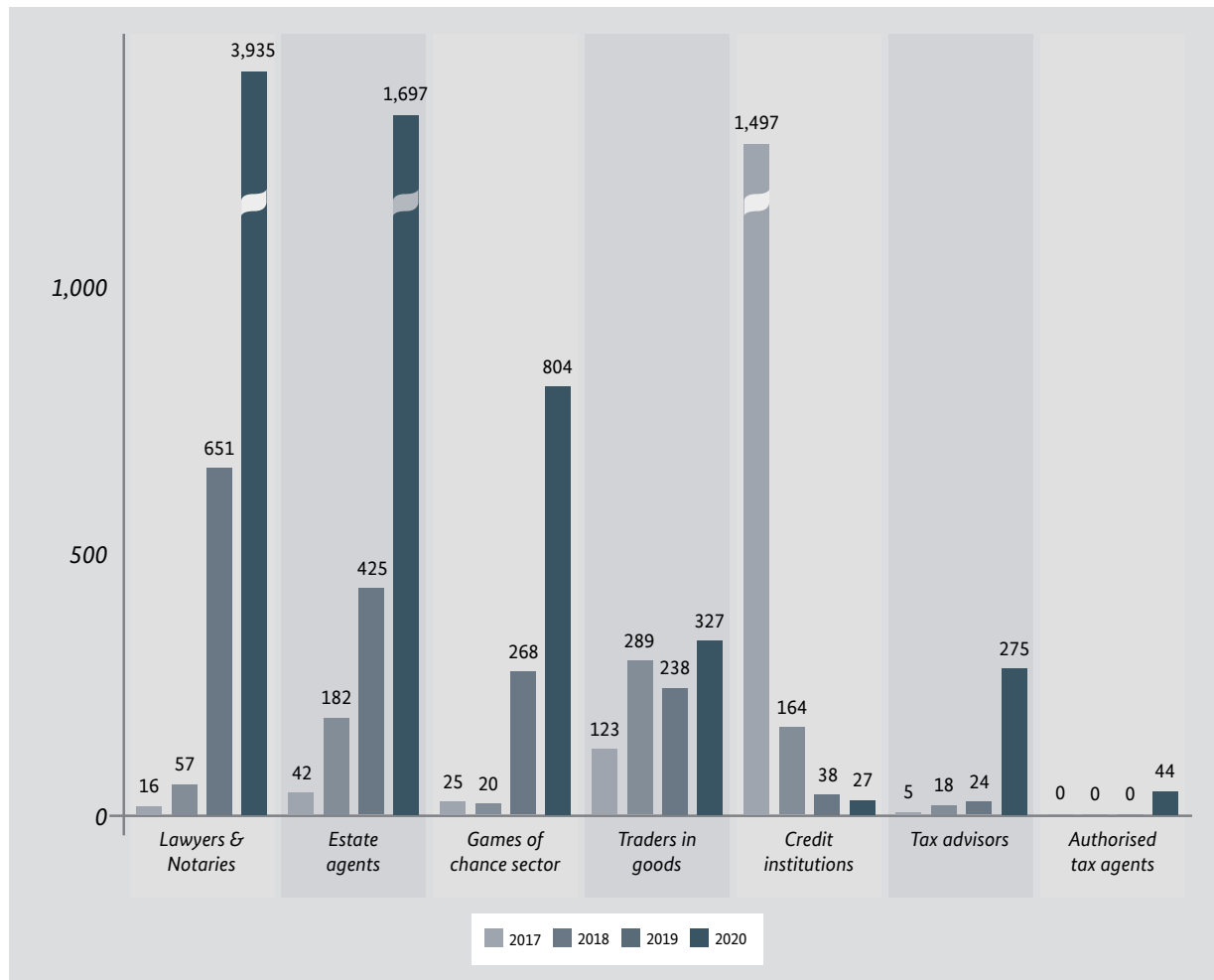


Figure 5: Registration Behaviour of Selected Subgroups of Reporting Entities

The largest share of the increase was accounted for by lawyers and notaries, whose registrations increased slightly more than six fold in relation to 2019. A total of 3,935 registrations were made by this subgroup of reporting entities in 2020. This accounts for slightly more than half of the new registrations in 2020.

Among estate agents there was an increase of 1,697 registrations, almost a fourfold growth compared to 2019 (425 registrations). After the registered reporting entities in the games of chance sector had already increased sevenfold to more than 300 reporting entities in 2019, there were 804 additional registrations in 2020. Thus, the total number of

registered reporting entities in the game of chance sector grew to almost 1,100 in 2020.

In the case of credit institutions, there were only 27 new registrations in 2020. Considering the total of 1,699 new registrations of credit institutions by the end of 2019, this represented an increase of just under 1.6%. The majority of credit institutions were already registered in 2017 when the electronic reporting system for money laundering STRs went into operation. Accordingly, no significant increase in new registrations is to be expected among credit institutions in the future.

Among traders in goods, the number of registered reporting entities increased from 650 to 977. Compared to previous years, no significant change in the registration behaviour of traders in goods can be observed. The sensitisation of this group of reporting entities in particular will be intensified and continued within the framework of money laundering conferences and expert lectures.

The largest increase in relative terms was among tax advisors and authorised tax agents. In 2019, only 47 reporting entities were registered in this area, whereas in 2020, 366 were registered.

Reporting entities also used the registration to gain access to the internal area of the FIU website

and to view the information published by the FIU (including typology papers). Thus, the existence of a suspicion in a specific case is no prerequisite of the registration of a reporting entity. In the FIU's view, the increase in registrations is not an indication of an increasing money laundering or terrorist financing risk, but rather of an increased awareness of those reporting entities obligated under the Anti-Money Laundering Act.

The number of registered reporting entities is thus different from the number of active reporting entities. The following table shows the number of reporting entities that submitted at least one report in 2020.

	Reporting entities	2018	2019	2020	Change 2019/2020
Financial sector	Credit institutions	1,232	1,274	1,290	↗
	Financial service institutions	53	87	90	↗
	Payment institutions and electronic money institutions	22	21	18	↘
	Agents	9	21	15	↘
	Independent business persons	0	0	0	→
	Insurance undertakings	41	57	51	↘
	Asset management companies	14	13	18	↗
	Total of reporting entities from the financial sector	1,371	1,473	1,482	↗
Non-financial sector	Financial companies	4	4	5	↗
	Insurance intermediaries	2	5	3	↘
	Lawyers	13	18	18	→
	Legal advisors who are members of a bar association	0	0	0	→
	Patent attorneys	0	0	0	→
	Notaries	5	15	723	↗
	Legal advisors	0	2	0	↘
	Auditors and chartered accountants	2	0	6	↗
	Tax advisors and authorised tax agents	3	4	11	↗
	Trustees, service providers for trust companies	1	4	4	→
	Estate agents	20	47	75	↗
	Organisers and brokers of games of chance	24	116	74	↘
	Traders in goods	146	174	164	↘
		Total reporting entities from the non-financial sector	220	389	1,083
	Total amount	1,591	1,862	2,565	↗

Table 2: Number of Active Reporting Entities

The number of reporting entities that submitted at least one report in 2020 increased again compared to the previous year. The number of active reporting entities in the financial sector changed only slightly in 2020, with an increase of nine active reporting entities. The minor fluctuations within the sector apply equally to all reporting entities. The increase of a total of 703 active reporting entities is mainly due to the non-financial sector, with

a growth of 694 active reporting entities. Particularly noticeable is the rise among notaries, which can be seen in connection with the entry into force of the Ordinance on reporting requirements in the Real Estate Sector under the Anti-Money Laundering (GwGMeldV-Immobilien) 1 October 2020. In addition, significantly more estate agents submitted at least one STR to the FIU in the reporting year.

Assessment Result for Suspicious Transaction Reports in 2020

Of the STRs received in 2020, a total of approximately 24,700 reports had been disseminated to the competent authorities by 31 January 2021¹². This corresponds to 17.2 % of the reports received in 2020.

	2019	2020
Suspicious Transaction Reports received	114,914	144,005
Of which disseminated by 31.01.2021 (rounded)	33,800	24,700
Rate of Dissemination	29.4 %	17.2 %

Table 3: Proportion of Suspicious Transaction Reports disseminated

For the previous year 2019, the rate of dissemination was 29.4%. Of the 114,914 STRs received in 2019, a total of just under 33,800 STRs were disseminated, also by 31 January 2021. The change in the rate of dissemination from 29.4% in 2019 to 17.2% in 2020 reflects the increased risk-based orientation of the FIU's working methods. Within the scope of performing its tasks and on the basis of the risk-based approach, the FIU concentrated on matters of value and forwarded them to the competent authorities in a targeted manner. However, it must be taken into account that the rates of dissemination for the two years shown could equalise somewhat in the course of 2021. This is due to the fact that in the course of 2021, more reports with a

date of receipt from 2020 will probably be disseminated than reports from 2019. The rates shown in the table above will be updated and adjusted in the 2021 annual report.¹³

The rate of dissemination is not only determined by the pure number of STRs; these may be disseminated in bundles. If the case analysis reveals sufficient indications of connections with money laundering, terrorist financing or other criminal offences, a bundled dissemination of all related STRs is made to the competent authorities. This is then counted as one dissemination. In 2020, a total of about 18,000 such analysis complexes were transmitted to the respective competent recipients.

The differentiation according to the recipients of the analysis reports disseminated shows that the majority - as in the previous years - was disseminated to the State Offices of Criminal Investigation (LKAs) and public prosecution authorities (StA). Their share has risen from a total of just under 90% in the previous year to 97.4%. On the other hand, the share of dissemination to all other addressees decreased. The share of dissemination to the main customs offices and customs investigation offices is now 1.5%. The tax investigation authorities still received 0.9% of all analysis reports. Other agencies, such as intelligence services or the Federal Criminal Police Office (BKA), received a total of 0.2% of the disseminations.

¹² The 31 January of the following year was chosen in order to also include reports that are received shortly before the end of the year and can thus only be processed in the following days.

¹³ In the previous annual reports, a distinction was made between monitoring and dissemination. Thus, for 2019, a ratio of 36% disseminations to 64% monitoring was calculated. The ratio was calculated on the basis of the final suspicious transaction reports (STR) processed in the respective year, regardless of their date of receipt. This approach, which has been communicated until now, was further developed after the introduction of the risk priorities and the increased risk-based approach of the FIU's work processes.

The adjacent figure shows a differentiation according to the recipients of the disseminations.

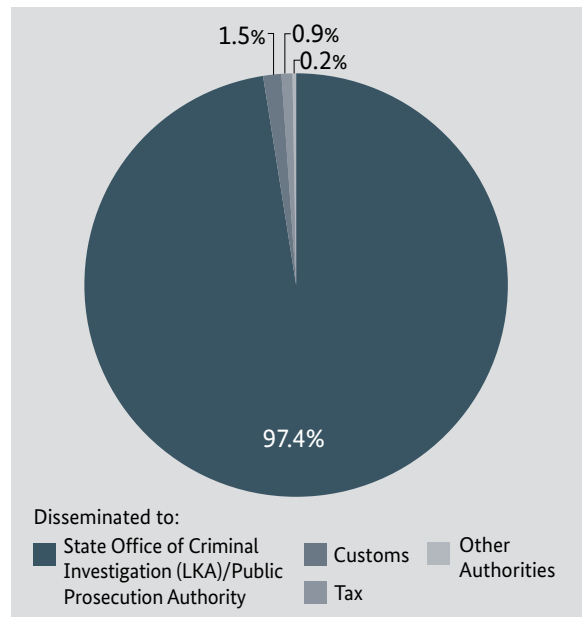


Figure 6: Breakdown of Reports by Recipients of Dissemination

In accordance with Section 8 of the Code of Criminal Procedure (StPO), the transmission of analysis results is based on the principle of residence. Analysis reports are thus always transmitted to the Law

Enforcement Agency (LEA) in whose district the place of residence of the (main) suspect or the seat of the (main) organisation involved is located.

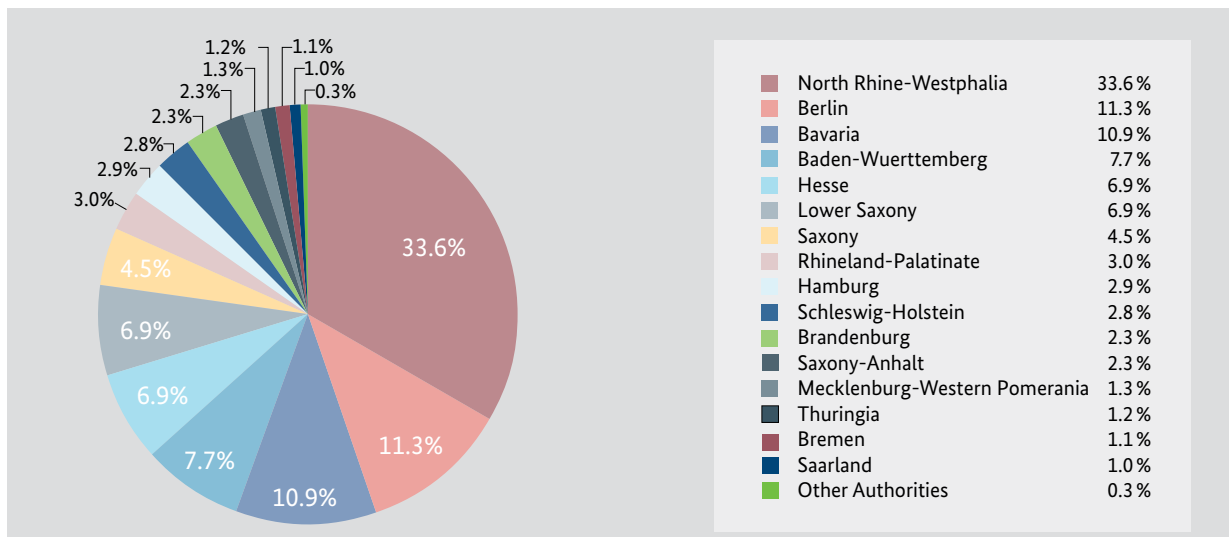


Figure 7: Distribution of the Disseminated Analysis Reports among the Federal States

In 2020, a total of 33.6% of the reports were disseminated to the federal state of North Rhine-Westphalia (share of population about 22%), followed by Berlin with 11.3% of the reports (share of population about 4%). The state of North

Rhine-Westphalia was particularly affected by disseminations related to the pandemic-related manifestations, especially Covid-19 emergency aid fraud. Of these disseminations, 43% were received by the federal state of North Rhine-Westphalia.

Feedback Reports from Public Prosecution Authorities

In 2020, the FIU received 12,618 feedback reports. Compared to the previous year, 4,947 fewer reports were received, which corresponds to a decrease of approximately 28%. With the FIU’s strengthened risk-based approach, significantly fewer analysis reports were disseminated to competent authorities in the reporting year, which also explains the decline in the number of reports received from public prosecutors.

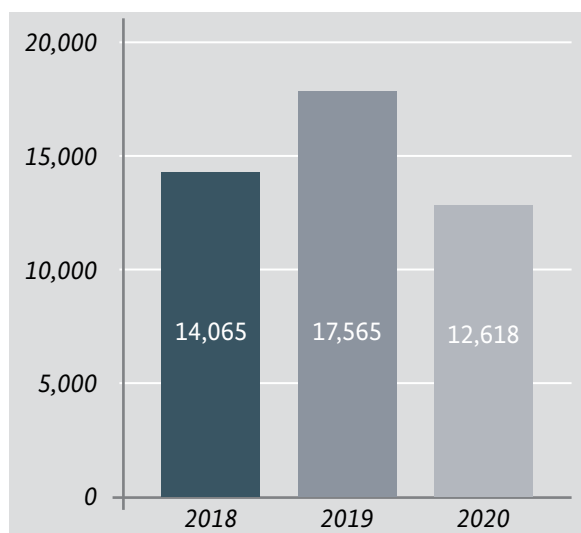


Figure 8: Number of Feedback Reports from Public Prosecution Authorities

A total of 783 of the feedback reports (6.2%) were convictions, penalty orders, decisions and indictments. The significant increase in this rate, which was 2.2% in the previous year, is mainly due to the successful fight against Covid-19 emergency aid fraud.

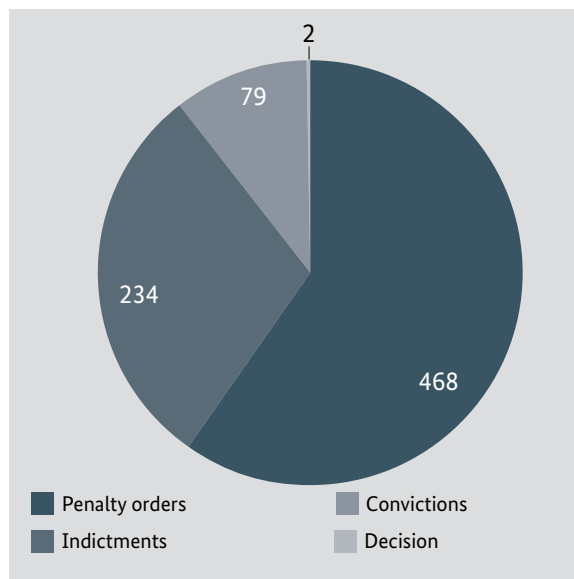


Figure 9: Overview of Convictions, Penalty Orders, Decisions and Indictments

In the feedback reports of verdicts and penalty orders transmitted in 2020, a conviction was handed down in at least 25% of the cases due to financial intermediary activity.¹⁴ In 8%, intentional money laundering offences were the basis for a conviction. In addition, there is an increase in the number of offences relating to various forms of fraud and thwarting foreclosure.

The high number of convictions due to the commitment of subsidy fraud according to Section 264 of the German Criminal Code (StGB) should be emphasised. 54% of the sentences and penalty orders transmitted in 2020 were issued due to this crime/offence. The offences were predominantly committed in connection with emergency aid granted due to the Covid-19 pandemic.¹⁵

¹⁴ Insofar as the feedback reports were assessable.

¹⁵ For further explanations in connection with emergency aid fraud, see the explanations on ‘Special Topic Covid-19’ in the section on ‘Typologies and Trends’.

Usually fines were imposed. If a fine was imposed, the average fine was about EUR 2,900; if a penalty order was issued, the average fine was about EUR 3,200. If a custodial conviction was imposed, the average sentence was 16 months. In 8 cases, a custodial sentence was pronounced by penalty order. In 34 cases, warnings were issued, with fines reserved within a probationary period. In a total of 346 cases, illegally obtained assets were confiscated.

In addition, two decisions were issued in independent confiscation proceedings under Section 76a of the German Criminal Code during the reporting period. On this basis, seized cash amounts can be confiscated if they stem from an unlawful act and the person affected by the seizure cannot be prosecuted or convicted for the underlying offence. The total amount of cash seized was just under EUR 38,000.

Unchanged from previous years, discontinuation orders, at approx. 93.8%, make up the majority of the feedback reports from the public prosecution authorities.

The proportion of criminal proceedings in connection with a STR that led to a conviction in 2020 may seem relatively low. However, it should be

noted that this is not a suitable criterion for measuring the effectiveness of the reporting system. According to the FIU's assessment, the relatively low number is due in particular to the challenging offence requirements for money laundering. For a conviction for money laundering under Section 261 of the StGB, not only the predicate offence must be proven, but also the money laundering activity and the origin of the object of the offence from the predicate offence. Furthermore, proving money laundering often does not lead to any 'added value' in terms of criminal proceedings. In cases where the perpetrator of the predicate offence is also the perpetrator of the money laundering, there is often a personal ground for exemption from punishment in accordance with Section 261, paragraph 9, sentences 2 and 3 of the StGB. But also in other cases, the additional conviction for money laundering often does not significantly increase the sentence. Against this background, a discontinued (money laundering) criminal case does not mean that the underlying STR is to be considered ineffective. In more than 80 orders for withdrawal of prosecution, it was explicitly stated that only the money laundering case was discontinued, but that the investigation of the predicate offence (e.g. fraud) was continued or the case was separated.

Case Study – Feedback from Public Prosecution Authorities¹⁶

Initial STR

A credit institution noticed that a customer, Mr. F, had deposited higher amounts of cash in his private account several times and was now apparently using the private account as a business account. When asked, the customer stated that the deposited funds originated from his self-employment, without, however, providing any further information or documentation. Due to the untraceable origin of the cash deposits, the bank filed a STR with the FIU.

FIU Analysis and Dissemination

In the course of the analysis carried out by the FIU, it was determined that Mr. F had committed criminal offences in the past, including money laundering and human trafficking for the purpose of sexual exploitation. Furthermore, there was a search alert for the investigation of his whereabouts. The case was disseminated to the competent State Office of Criminal Investigation (LKA).

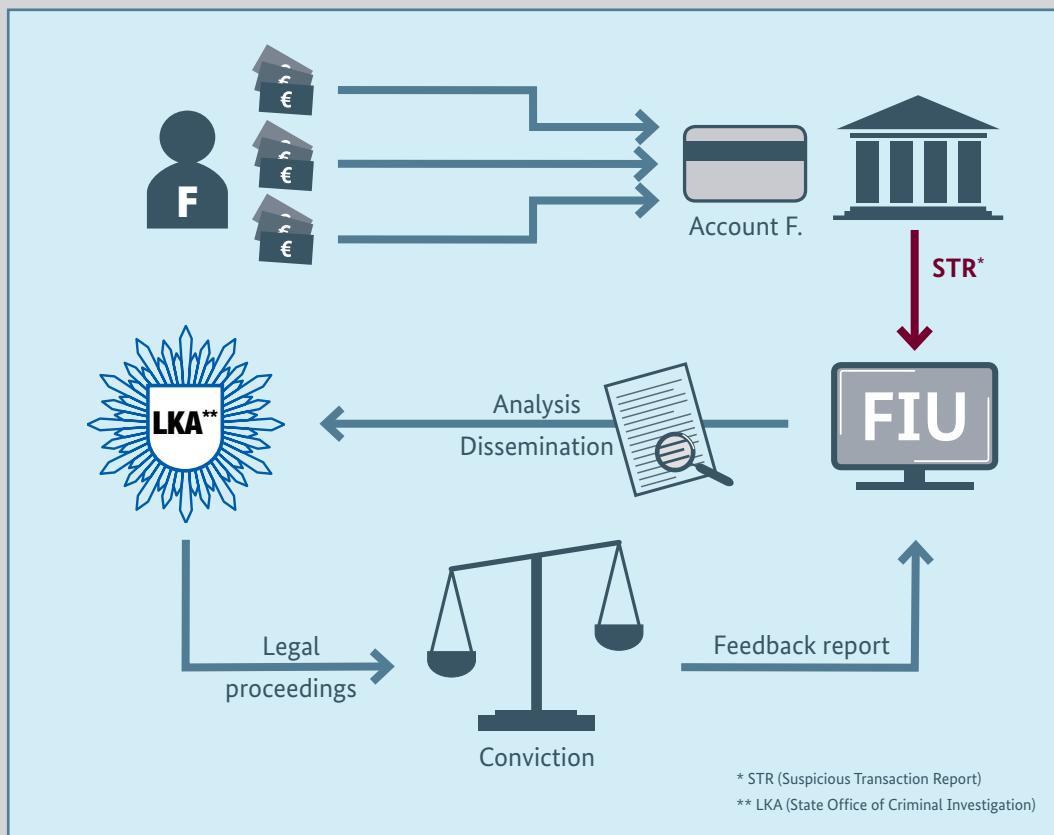


Figure 10: Case Study – Feedback Reports from Public Prosecution Authorities

16 The case study presented is a real case from the FIU's practice.

Investigations and Conviction

The court was convinced that Mr. F brought a large number of foreign women to Germany or had them brought there in order to lead them into prostitution despite their lack of residence permits. At Mr. F's behest, the women were subsequently forced to hand over part of their earnings to a third party, who sent part of the money, untaxed, to Mr. F via a money transfer service. In this way, the third party also transferred money to other third parties in other EU countries, who then handed over the amounts received to Mr. F.

Mr F. was sentenced to a total term of imprisonment of one year for money laundering. Insofar as Mr. F. could be charged with further offences in the present proceedings, further criminal prosecution was discontinued because of convictions that had already taken place abroad as well as according to Sections 154, 154a of the Code of Criminal Procedure (StPO).

Temporary Freezing Orders

By means of a temporary freezing order, the FIU can prohibit the execution of a transaction if there are indications that a transaction is related to money laundering or serves the financing of terrorism. This gives the FIU the opportunity to follow up on indications and analyse the transaction until a final assessment of the facts has been made, without removing incriminated funds from the state's sphere of influence through cash withdrawals or transfers. The FIU has an important and effective tool to prevent money laundering through the possibility of issuing a temporary freezing order, whereby the need to carry out a temporary freezing order is carefully weighed in each individual case.

In the reporting year, the FIU issued 14 temporary freezing orders. Transactions with a total volume of approximately EUR 1.4 million were stopped for up to 30 days. In the case of eight national temporary freezing orders, the further analysis of each order revealed concrete facts that led to the dissemination of the case to the competent authority.

Within the framework of international cooperation with foreign FIUs, a total of six temporary freezing orders with a transaction volume of approximately EUR 730,000 were successfully carried out through incoming requests.

Case Study – Temporary Freezing Order¹⁷

Based on a request from a foreign FIU and the analysis of a STR (1) received from bank A, there were indications that an account held at bank A was being used to receive transactions or transfers of incriminated funds and forward them to other accounts. Payments totalling around EUR 120,000 were received in the corresponding account at bank A from foreign accounts of companies T and E (2). Immediately after receipt of payment, three transfers of this amount, each amounting to EUR 30,000 and EUR 32,000 respectively, were further transferred to an account at bank B (3). The FIU's analysis showed that the payments were incriminated funds from fraudulent acts to the detriment of the two companies T and E, which were based abroad. According to the bank statement for the account at bank B, the managing director J of company G also made a cash deposit of EUR 30,000 on the same day (4). Together, the transfers with the cash deposit resulted in a total sum of EUR 122,000. On the next day, a total sum of EUR 123,000 was transferred in favour of the account Z in an Eastern European third country of the company W based in the EU (5). The alleged purpose of the payment was the purchase of a high-priced car. Further analyses revealed that the managing director J of company G had already been investigated for money laundering (6). The FIU Germany also had information that pointed to irregularities in the import of luxury cars from an Eastern European third country.

¹⁷ The case study presented is a real case from the FIU's practice.

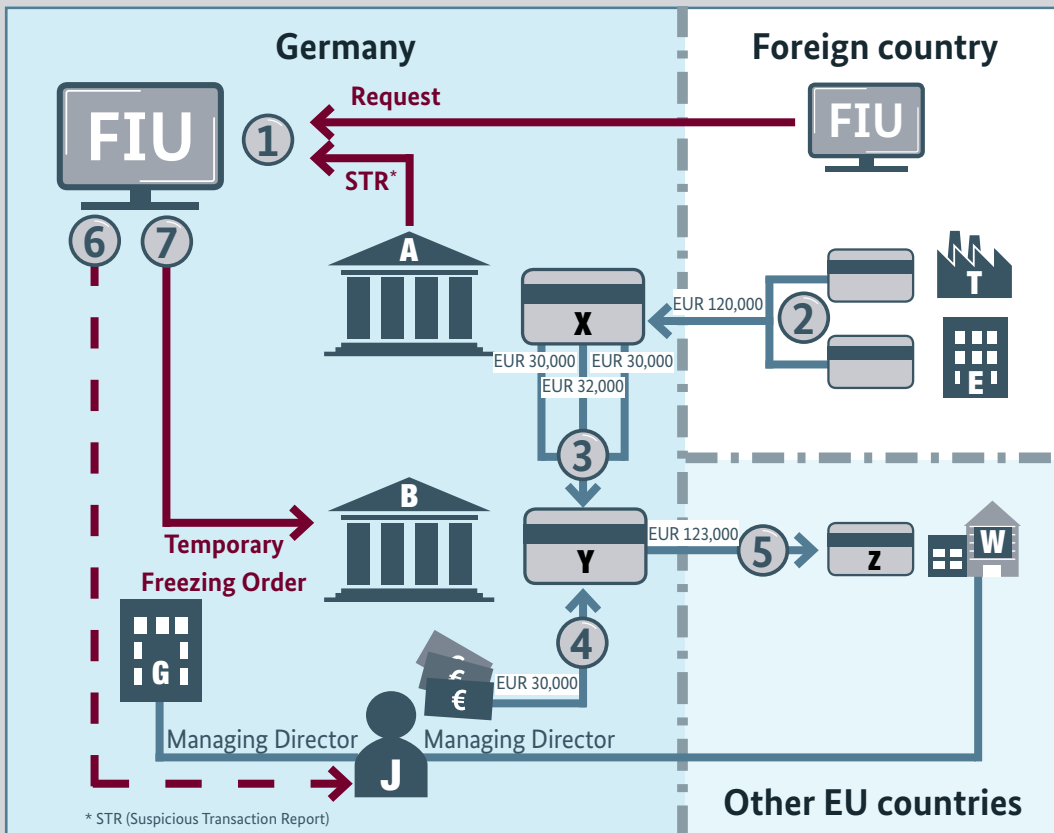


Figure 11: Case Study – Temporary Freezing Order

The FIU then issued a temporary freezing order pursuant to Section 40 (1) AMLA to seize EUR 92,000 in the account at bank B and to conduct further analyses in this case (7). According to information from a foreign FIU, as well as through his own research, it could be established that Mr J is also the managing director of company W. Further analyses, including information from another foreign FIU, confirmed that company W is in turn the account holder of account Z in the Eastern European third country. The case was handed over to the competent public prosecution authorities. The latter obtained a seizure order from the competent district court and then implemented this with an attachment order for the account at bank B.

One temporary freezing order was related to terrorist financing or state protection. The total volume of this temporary freezing order was just under EUR 39,000. The temporary freezing order was taken against the background of a STR which contained indications that the person belonged to the Salafist scene and was involved in illegal fundraising, which was presumably used to finance terrorism. The STR was processed in the light of

the key risk area on misuse of NGOs/NPOs. In addition, there were references to proceedings conducted by the Attorney General as well as to proceedings conducted by the Federal Ministry of the Interior, for Building and Community to ban associations. The case was handed over to the competent LEA authority after the FIU analysis was completed.

Case Study – Temporary Freezing Order: Potential affiliation to the Salafist scene¹⁸

A person initiated a large transfer from his PayPal account to his own current account, which was disproportionate to the account holder's usual lifestyle and income. A short time later, the customer informed the account-holding institution that he wanted to have the amount paid out in cash. When asked, the client stated that he had initiated a fundraising campaign for a charitable organisation. Since the association could no longer keep accounts in Germany due to doubts about its non-profit status, the client had acted on behalf of the association and made his private accounts available. He now wanted to give the advised cash amount to 'people in need'. As the bank refused this transaction, the client demanded that the money be transferred to another account. This was also refused by the bank. The bank blocked the account and a STR was submitted to the FIU.

FIU Analysis and Dissemination

The FIU issued a temporary freezing order on the account in question because of the potential connection to an apparently abusive association. In addition, a request for information was sent to a European partner authority in order to obtain further information on the origin and use of the funds. After responding to the request for information, the client's statements to the bank were confirmed and an actual connection to the association in question was established. Criminal proceedings are currently pending against the association by the Federal Prosecutor General on suspicion of terrorist financing pursuant to Section 89 c of the German Criminal Code (StGB), as well as proceedings by the Federal Ministry of the Interior, for Building and Community to ban the association. In addition, it was established that the total amount of the donations declared by several clients and transferred to the PayPal account corresponded to the amount transferred to the client's current account in Germany. Taking into account the overall facts of the case, it could therefore not be ruled out that the funds were passed on to the involved association in cash and were intended to serve a possible financing of terrorism. The analysis report with the above-mentioned research results was subsequently disseminated to the competent State Office of Criminal Investigation.

¹⁸ The case study presented is a real case from the FIU's practice.

Proliferation Financing

Proliferation refers to the spread of weapons of mass destruction, in particular nuclear, biological, chemical and radiological weapons, including their launcher systems, technologies, know-how and the materials or components required for their production. Strict legislation and effective export controls are indispensable in Germany, as various risk states continue to rely on the world market for the research and production of weapons and launcher systems, despite considerable technical progress in some cases.

In addition to the incoming STRs, indications of proliferation financing also stem from communications by the intelligence services and from reports by foreign authorities. When processing individual cases, the FIU is in close contact with the Customs Investigation Service (ZFD), in particular the Customs Criminological Office (ZKA). The prevention and combating of proliferation financing is carried out within the framework of international standards, which aim to uncover or prevent the distribution or spread of the aforementioned goods, technologies and know-how. Despite strict existing export controls, Germany

can be the target of procurement efforts by risk countries. In particular, the processing of transactions and the related disguised transaction channels are diverse and subject to constant change in order to circumvent export control procedures. The analysis of STRs and in particular the financial flows contained therein can thus serve, among other things, to identify proliferation-promoting activities at an early stage – in addition to already existing export control procedures.

Possible circumventions of legal export regulations exist, for example, in the inclusion of unencumbered companies, persons or state institutions (e.g. universities) as recipients of a delivery or the processing of transactions via unsuspecting third countries.

A total of 34 STRs were submitted to the FIU in the reporting year that contained indications of a possible proliferation or embargo/sanctions background. In this context, references to Iran, North Korea, Lebanon and Iraq, but also Russia were identified. In the previous year, 26 corresponding STRs were received.

Transactions

Most of the STRs that are received by the FIU contain suspicious transactions which constitute an important component of detecting money laundering activity. A transaction is the transfer of assets between two parties, usually using a credit institution or a financial service provider. The transfer of crypto assets between electronic purses also constitutes a transaction. Further examples are bank transfers, cash withdrawals from current accounts, cash transactions of any kind or the cashing of chips in casinos. A STR does not necessarily have to contain a transaction, but a large number of transactions can be reported in a single STR. Therefore, the number of STRs received is not directly comparable to the number of transactions transmitted.

In the reference period 2020¹⁹ the FIU received reports of around 481,000 suspicious transactions, around 35% more than the previous year.

The proportion of German domestic incidents rose from approx. 37% in the previous year to around 50% of all transactions. In contrast, the proportion of transactions from or to Germany, i.e. which show Germany as the country of origin or destination remained almost the same with 36%. Only 4% of the transactions have no reference to Germany (2019: 6%). This can, for example, be the case for correspondence banking activities in which the reporting credit institution is a reporting entity in Germany but acts exclusively as a service provider for settling cross-border transactions. For 10% of the transactions there is no information about the country of origin or destination.

For a national analysis, transactions from and to Germany are particularly relevant. The following figures show the severity of the reported transactions that Germany was involved in as the country of origin or destination.

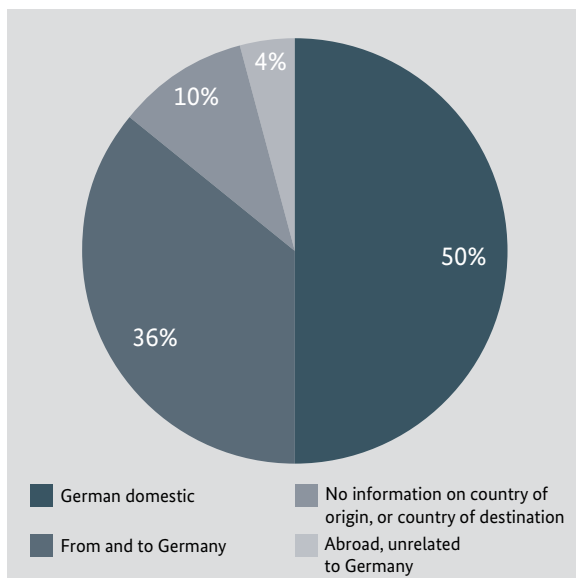


Figure 12: Foreign Involvement in Suspicious Transactions

¹⁹ This number may increase after the preparation date of the annual report if further STRs containing transactions that were executed in 2020 are received in subsequent years.

Suspicious Transaction Reports

Transactions

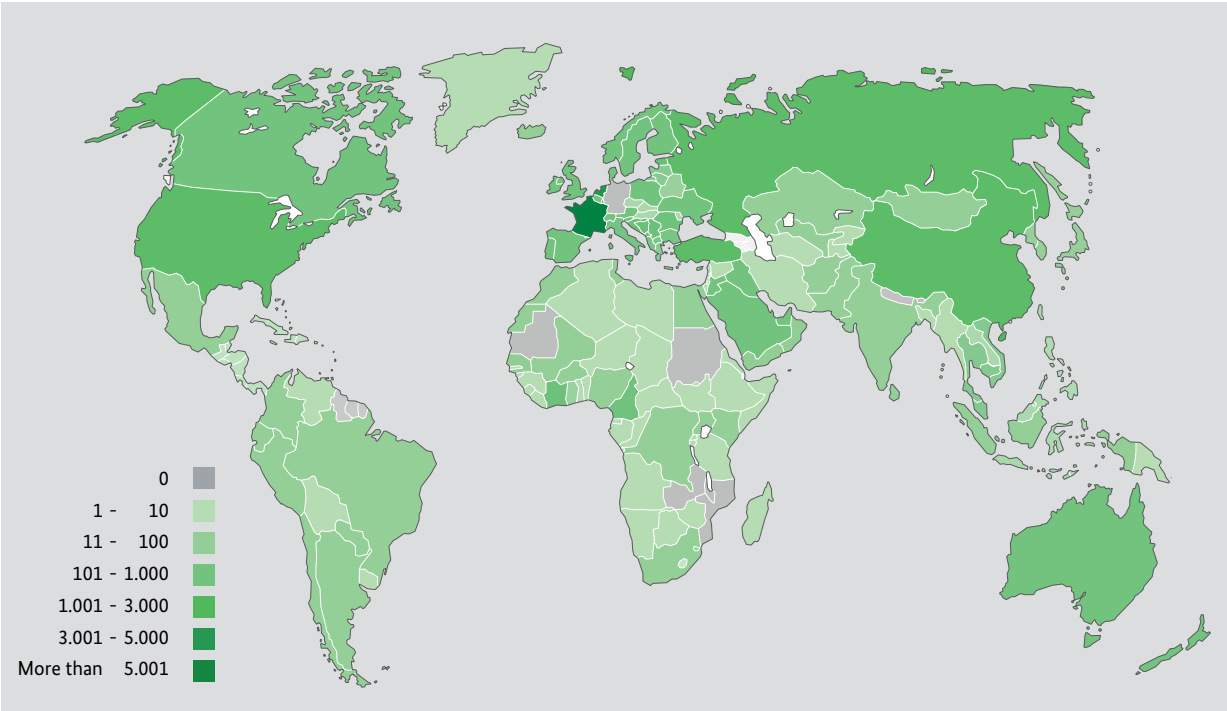


Figure 13: Number of Suspicious Transactions by Country of Origin

In 2020, over 43,000 suspicious transactions were received by Germany (2019: just under 31,000). When looking at the transactions according to their countries of origin, France stands out with over 5,300 transactions as well as the Netherlands with over 4,300 transactions. As in the previous year, suspicious transactions that had Germany as their destination come primarily from Western European countries (between 1,500 and 2,900 transactions each), Turkey and the major economies of China, Russia and the USA (between 1,000

and 1,500 transactions each). With over 2,200 transactions with Estonia as the country of origin, there was a sharp increase, which in the context of the developments surrounding the Estonian subsidiary of Danske Bank suggests an increased sensitivity on the part of the reporting entities. Increases were also noticeable in Malta (more than quadrupled to almost 1,000 transactions) and Lithuania (more than tripled to almost 1,000 transactions).

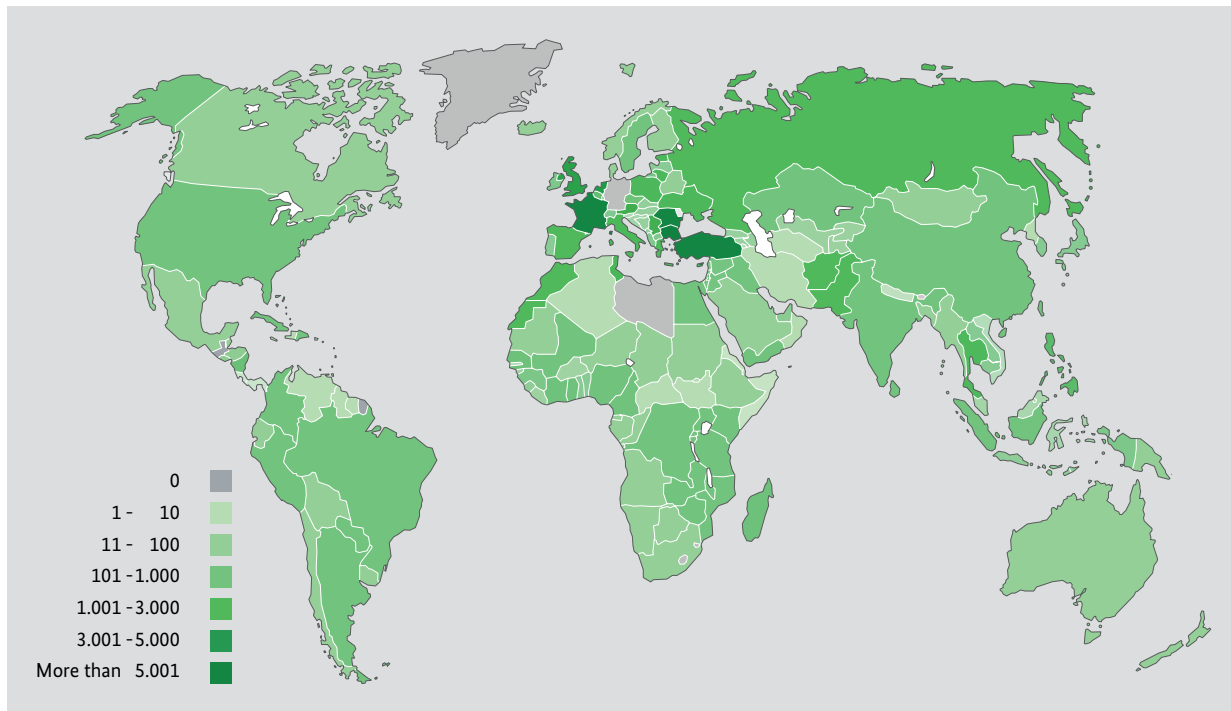


Figure 14: Number of Suspicious Transactions by Country of Destination

An even greater increase than the number of incoming transactions to Germany was experienced in the number of outgoing transactions from Germany. With over 133,000 transactions, an increase of around 44% was recorded here compared to the previous year. As in the previous year, the focus in this category is on Turkey as the country of destination (almost 26,000 transactions). Besides France (almost 6,800 transactions), the countries of Eastern Europe play a major role. With Bulgaria

(around 8,200), Romania (just under 6,800), Albania (around 4,600) and Serbia (around 4,100), four of the six highest-ranking countries can be assigned to the Eastern European region. Albania showed a particularly high rate of increase compared to the previous year, with a nearly fivefold increase in transaction volume. High growth rates of almost 200% were also recorded for transactions to Great Britain (around 3,100), Thailand (almost 2,400) and Pakistan (around 2,000).

Typologies and Trends

Description and Continuation of Key Risk Areas

Special Topic Covid-19

Key Risk Area Trade-Based Money Laundering

Key Risk Area Commercial Fraud

Key Risk Area Use of New Payment Methods

Key Risk Area Misuse of NGOs/NPOs

Typologies and Trends

Description and Continuation of Key Risk Areas

Based on the key risk areas as defined for the first time in the summer of 2019 with the participation of the LEA, the FIU consistently continued the risk-based approach of its processes in the reporting year 2020 and further improved the effectiveness of its filter function as provided for by law.

Since the beginning of the year, every piece of information received by the FIU – and thus in particular suspicious transaction reports (STRs) pursuant to Sections 43, 44 AMLA – is continuously evaluated on a risk basis to determine whether it requires further analysis within the meaning of the FIU’s legal core mandate. At the beginning of the analysis process, incoming STRs are automatically reconciled with relevant data sources/files and pre-filtered in a semi-automated

manner based on the defined key risk areas (risk-based approach, RBA). STRs that are not initially filtered out during this process remain in the so-called monitoring phase alongside the risk-based analysed reports and are continuously compared with the new information received by the FIU. By this, these STRs are constantly included in the analysis process and thus made accessible for repeated evaluations.

The applied key risk areas take into account both sector-related and phenomenon-related risks. In general, a distinction is made between the areas of money laundering and terrorist financing, but a common key risk area is also set with the use of new payment methods as a result of new technologies.

Key Risk Areas Money Laundering



Real Estate

Real Estate carries a high risk of money laundering. Sales generally involve high transaction volumes. In addition, there is a wide range of options in legal arrangements for potentially concealing the origins of the funds and the ownership structures, also by involving national and foreign legal entities. As an asset, real estate is considered to be a stable investment that is independent from economic cycle. Since it is tied to a specific location and can only be substituted under certain conditions, it is thus considered the most significant investment property in Germany.



Use of Cash (when procuring high-value goods)

Trading valuable goods is characterised by the use of large sums of cash, which facilitates the anonymous transfer of larger sums of money. In addition, non-regulated and informal business practices in these markets enable funds from criminal activities to be integrated into the legal economy. The acquisition of motor vehicles, art and antiques and other luxury goods is the focus here.




Trade-Based Money Laundering

Trade-Based Money Laundering (TBML) takes advantage of the complex nature of the flows of goods and money in international commerce. Over- or under-invoicing, charging for goods and services multiple times, fake deliveries with content that deviates from the description or incorrect descriptions, involvement of third parties or usage of shell companies are typical scenarios here. Germany is a strong exporter and importer of goods and is thus considered particularly ‘attractive’ for this typical method of money laundering.




Games of Chance / Betting

The gambling industry also offers methods for concealing the origins and further use of the funds involved, i.e. through its established diversified online market. A high circulation velocity and the use of cash below the legal identification limit of EUR 2,000 increase the gambling sector’s susceptibility to money laundering.




Organised Crime in the Form of Clan Crime

Organised crime represents a focus of interest in the fight against crime in Germany. Organised perpetrator structures and large-volume profits resulting from illegal business must be laundered so that funds can be integrated into the legal economy. With this context, foreign extended families are the current particular focus of the LEA's attention and of their police investigations.



Serious (Tax) Criminal Acts e.g. Carousel Fraud


Trade across the borders between two EU Member States can result in the right to a tax refund due to the structure of VAT legislation. Carousel fraud often exploits this in large-scale, cross-border tax fraud operations. By the time the responsible tax auditor becomes aware of the tax evasion, the companies involved often no longer exist.



Commercial Fraud

As a predicate offence to money laundering, commercial fraud occurs primarily in connection with Internet fraudsters who exploit account opening procedures for themselves and use them, for example, to operate fake shops or to forward funds in connection with love scamming activities. Forms of commercial fraud are also carried out by misusing the identity. However, the so-called identity theft is not a mandatory criterion for a commercial form of this method; rather, it is always aimed at obtaining a continuous source of income from a repeated commission of the offence.


Key Risk Area Regarding Terrorist Financing and Money Laundering



Use of New Payment Methods


The continued (technical) development of payment methods goes hand in hand with a significant acceleration in the speed of transactions, e.g. due to instant payments via apps and smartphones. Using virtual assets for making payments is also included within this subject. For the relevant processing platforms and/or electronic payment systems, tracing transactions is difficult or even impossible due to the regularly applied encryption techniques and internet-based transmission paths. In light of this, these platforms and systems are susceptible to becoming vehicles for acts of money laundering and terrorist financing purposes.

Key Risk Area Regarding Terrorist Financing



Misuse of NGOs/NPOs

Non-Governmental Organisations (NGOs) and Non-Profit Organisations (NPOs) are held in high regard by society. They often act across country borders and have a large amount of financial resources, which makes them interesting to those seeking to finance terrorism. On the one hand, funds can be (partly) misappropriated to terrorist organisations. On the other hand, alleged charities might be completely controlled by terrorist groups so that the funds can be used entirely for terrorist purposes.



Misuse of Money and Value Transfer Services

The settlement of transactions via financial transfer service providers can also be abused with a view to financing terrorism. Specifically, cross-border transactions are subject to a higher level of risk if the country of destination is defined as a high-risk country. Here, the risk is that the sums of money will be transferred to conflict zones and will be used for terrorist purposes there.

Figure 15: FIU Key Risk Areas

As a control and prioritisation instrument, the FIU continuously checks the validity of the introduced key risk areas, both in consideration of the development of crime in Germany as well as ad-hoc. This means that any necessary adjustments can be made at any time, which have a direct impact on

the operational analysis activities. In 2020, the key risk areas of commercial fraud and identity theft involving LEA was revised and the previous additional criterion 'identity theft' was deleted without replacement.²⁰

Ad-hoc Adjustment of Case Prioritisation due to Pandemic-related Crime Developments

Another concise example regarding an ad-hoc adjustment in case prioritisation in the reporting year 2020 was the crime developments observed in Germany in connection with **Covid-19 emergency aid payments** and the increase in STRs related to these. Subsidy fraud is not originally a key risk

area of the FIU. However, the FIU reacted to the changes in the crime scene and formed an additional focus of its work in order to be able to disseminate related STRs directly to the competent LEA.²¹

Covid-19 Emergency Aid Payments

In April 2020, the German government adopted a 50 billion euro aid programme that provided emergency aid to small businesses, the self-employed and freelancers. In order not to jeopardise the economic existence of the applicants and to bridge acute liquidity bottlenecks due to ongoing operating costs, this aid programme provided one-off, non-repayable grants. In the course of the year, further similar aid programmes were set up.

Subsequently, various fraud attempts became apparent in the context of the Covid-19 emergency aid payments, which directly influenced the FIU's reporting volume considerably. In particular, the FIU received numerous STRs in this context that contained indications of wrongfully obtained Covid-19 emergency aid payments.

²⁰ For more details on the adjustment of the key risk area on commercial fraud, see 'Key Risk Area Commercial Fraud' later in this section.

²¹ For further discussion in relation to Covid-19, see 'Special Topic Covid-19' later in this section.

Special Topic Covid-19

Immediately after Covid-19 started to spread in Germany from the beginning of March, criminals adapted their patterns and approaches to the new situation and specifically exploited fears and concerns of the population during the pandemic.

Thus, the year 2020, especially the months of April to August, was marked by the effects of the Covid-19 pandemic. This applied both to the total number of reports and to the type of reports. From

mid-March to the end of December 2020, the FIU received around 11,200 suspicious transaction reports (STRs) that were possibly related to Covid-19. Of these, 26 reports were related to the phenomena of terrorist financing and other crimes relevant to state protection. The following figure shows the development of the received STRs with reference to Covid-19 in the course of the reporting year.

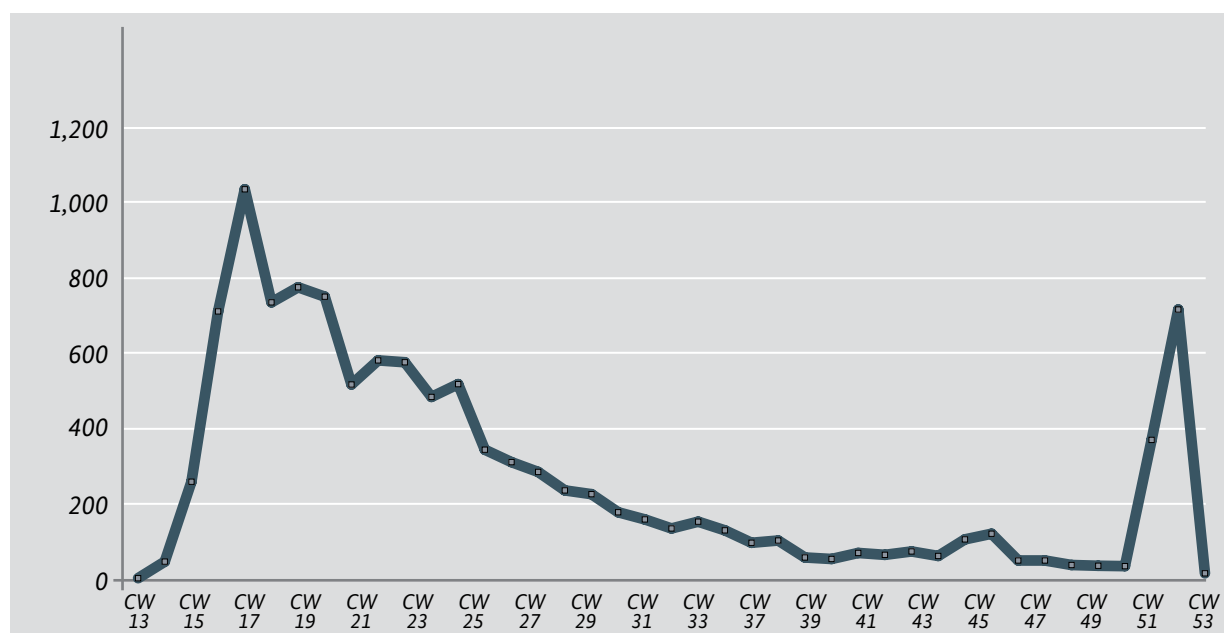


Figure 16: Received Suspicious Transaction Reports with reference to Covid-19

After an initial sharp increase, a downward trend is discernible. At the end of the year, dedicated analysis projects carried out by reporting entities led to a renewed temporary increase in the number of Covid-19-related reports submitted to the FIU.

In order to counter this new development effectively, it was necessary to quickly provide reporting entities, in cooperation with the national authorities and international partners, with

suitable assistance in identifying relevant constellations. For this reason, as early as May 2020, the FIU published a clues and typology paper on its website. The publication described the main types of criminal activities in connection with the Covid-19 pandemic as well as it provided corresponding instructions for reporting entities. It was then adapted accordingly in the course of the year as new information became available. In order to stay up to date with the very dynamic development of various forms of financial crime,

especially in the first weeks of the pandemic, the staff of the FIU maintained a lively exchange with various international organisations. An important focus of the strategic analysis was the preparation of regular internal status reports.

In the following, selected facts will illustrate the spectrum of criminal activities in the area of money laundering and terrorist financing in connection with Covid-19.

Fraud in connection with the Application for and Disbursement of Emergency Financial Aid

Around 9,500 of the STRs submitted to the FIU in connection with Covid-19 related to the fraudulent application for emergency aid. At times, these reports accounted for up to 25 % of the total number of reports.

In the spring of 2020, criminals attempted to obtain emergency aid for businesses and freelancers through various methods. In a number of cases, businesses had applied for emergency aid without justification, even though their economic situation had not deteriorated, they had been founded solely for the purpose of the unauthorised application, or they had already been bankrupt or in liquidation. In some cases, these were companies with connections to organised crime groups.

Furthermore, private individuals who had not registered a business often applied for emergency aid. Some of these were recipients of social benefits who were tricked by criminals into providing their account details in return for payment of a 'premium'. This also happened in combination

with fake websites on which claimants had entered their data, believing that it was the legitimate website of a federal state. In this way, criminals were able to tap the company data entered in good faith and have financial intermediaries use them as pay-out accounts. In this case, the named payee and the actual account holder often differed from each other.

In most of these cases, the amounts paid out were disposed of promptly, for example through cash withdrawals, transfers abroad, forwarding to trading platforms for crypto assets or the settlement of seizures. This involved both single perpetrators and criminals who act in concert.

The decentralised payment of emergency aid and the initially very unbureaucratic application process favoured such constellations. These reports were transmitted to the LEA via a separate, i. e. simplified procedure.

Case Study – Emergency Aid Fraud I²²

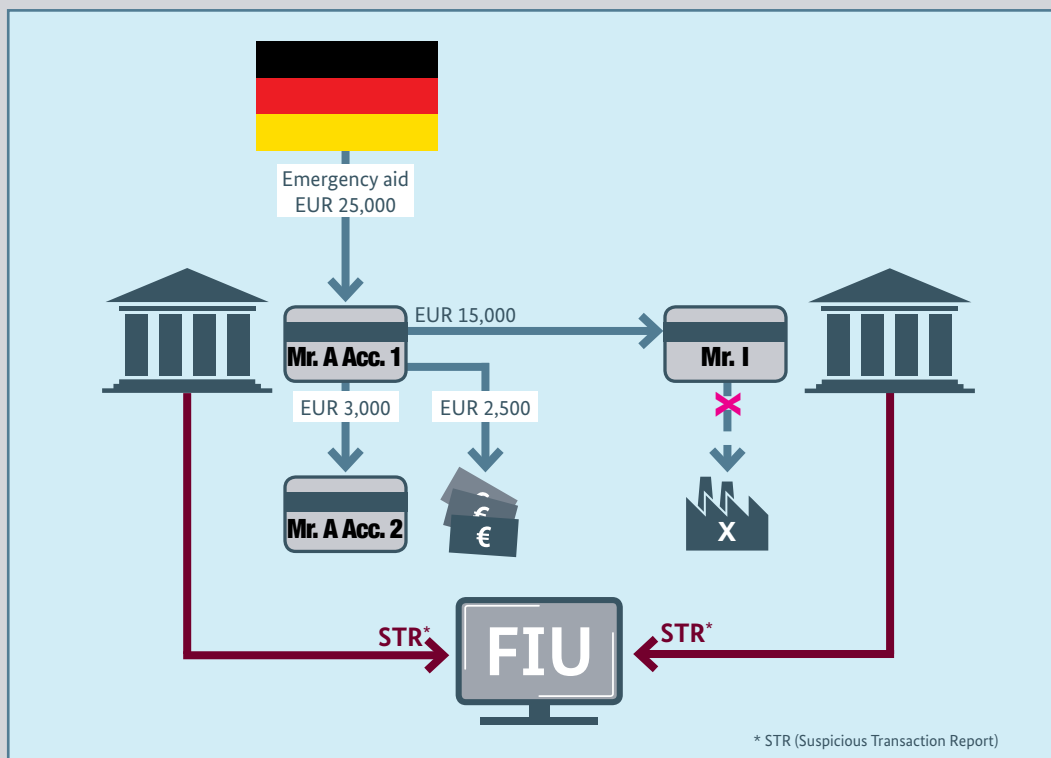


Figure 17: Case Study – Emergency Aid Fraud I

Initial STR

A credit institution reported that private client A had received EUR 25,000 in Covid-19 emergency aid to his account, although it was not known that the client was self-employed. Of this amount, EUR 3,000 were transferred on the same day to another current account of the account holder, another EUR 2,500 were disposed of in cash. The client transferred EUR 15,000 to the overnight deposit account of his relative I with the purpose of use 'Covid-19 emergency aid refund'. This amount was then to be forwarded to a company X with purpose of payment 'Investment 2020'. The bank of the relative I also reported the facts, whereupon the reports were combined in the FIU for further analysis.

22 The case study presented is a real case from the FIU's practice.

FIU Analysis and Dissemination

The FIU's analyses revealed that private individual A had applied for the emergency aid because he runs a snack bar as his main occupation. However, the documents of the competent tax authorities showed that he was running the snack bar as a side-line. It also turned out that he had overstated the number of employees in the emergency aid application form in order to receive a higher amount of emergency aid. Investigations also revealed that the managing director of Company X was not listed for tax purposes and did not receive a salary. In addition, he had submitted funds from a robbery offence to the German Federal Bank for exchange and had also applied for Covid-19 emergency aid for his business. The facts of the case were forwarded to the public prosecution authority on suspicion of fraudulent obtaining of the emergency aid. This ordered a freeze on assets, i.e. the amount was blocked for further disposals.

Case Study – Emergency Aid Fraud II Clan²³

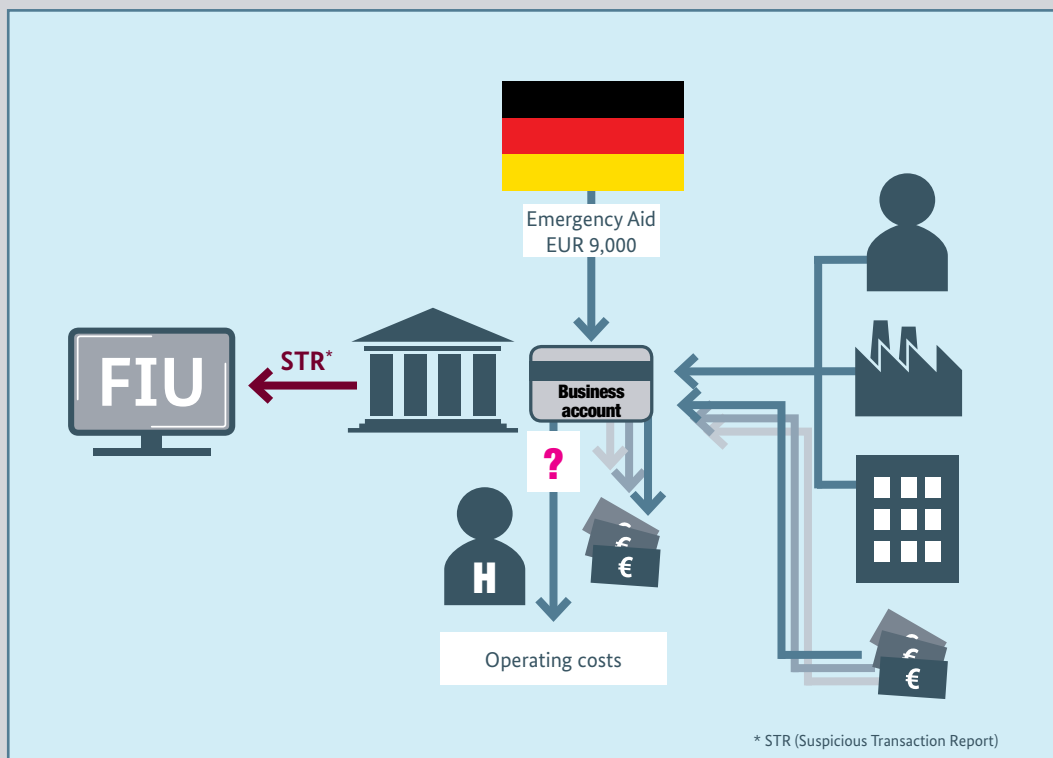


Figure 18: Case Study – Emergency Aid Fraud II

Initial STR

A credit institution reported person H, who held a business and a private account there. Information was available which indicated a connection to the clan milieu. In the past, the business account of person H had shown invoice credits from a private person and two companies, which did not allow any conclusion to the services rendered. On the whole, the account did not show any regular business-typical activities such as wages, social security contributions or material purchases. Instead, the credited amounts were frequently withdrawn in cash. In addition, there were frequent cash deposits of which the origin was unclear. Person H had applied for Covid-19 emergency aid and received EUR 9,000 in this context. It was not clear whether these funds were used to cover operating costs or whether an economic emergency existed at all.

23 The case study presented is a real case from the FIU's practice.

FIU Analysis and Dissemination

An analysis by the FIU revealed that person H, together with another private individual, had founded another company in May 2020, for which Covid-19 emergency aid had also been applied for and paid out. It was determined that person K was simultaneously employed and that the Covid-19 emergency aid had therefore been fraudulently obtained. The emergency aid money had been used to settle private debts.

The facts of the case were forwarded to the public prosecution authority on suspicion of fraudulent obtaining of the emergency aid. The prosecution ordered a property arrest in the amount of the disbursed sum.

Pre-payment Fraud in connection with Fictitious Offers for Protective Masks and other Medical Products

Another modus operandi emerged at the beginning of the Covid-19 pandemic in connection with offers for protective masks and other medical products. For example, protective clothing and disinfectants, which were in short supply, especially in the spring, were offered for sale on the Internet. However, despite receipt of payment,

the goods were not delivered.²⁴ The reported cases involved both one-off actions by perpetrators as well as such that were connected to each other and for which it could be assumed that they were committed by a gang. In the latter case, financial intermediaries were engaged as recipients of the purchase payments.

Trade-based Money Laundering

The method of TBML, in which money is laundered through goods by over- or under-invoicing, false declaration or false declaration of quantities, among other things, was also adapted to the

situation under Covid-19.²⁵ Protective clothing, masks or other medical products were used as underlying goods.

²⁴ See also the case study 'Fraud Involving Covid-19 Protective Masks' in the section 'International Cooperation'.

²⁵ For more information on the key risk area of TBML, see the explanations under 'Key Risk Area Trade-based Money Laundering' later in this section.

Case Study – Trade-based Money Laundering²⁶

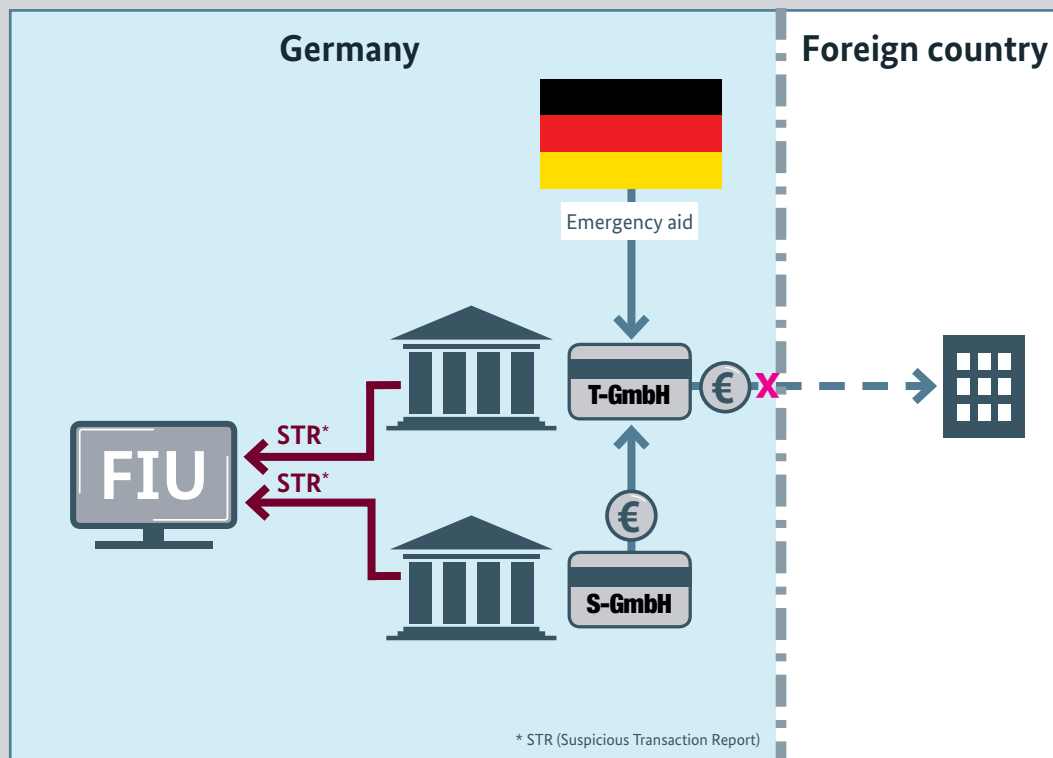


Figure 19: Case Study – Trade-based Money Laundering

Initial STR

A credit institution reported the account of T-GmbH for which high increases in turnover were identified, although Covid-19 emergency aid had already been applied for and had been paid out to T-GmbH. When asked, T-GmbH explained that protective masks were imported from Asia and then sold on to S-GmbH. The original business field of T-GmbH comprised general organisational services for third parties as well as internal transport, handling and storage processes. In the course of the business relationship, however, the managing director stated that the company traded in special items which were often purchased abroad and then sold for cash. The invoices submitted for the purchase of protective gear from the Asian supplier did not match the invoices submitted for the sales from T-GmbH to S-GmbH in terms of amount and date. It was therefore unclear whether and for what amount the goods had been sold by T-GmbH to S-GmbH. The payments received by T-GmbH also did not match these invoices. Whether the deliveries for protective equipment actually existed remained unclear.

An outgoing foreign transfer of EUR 1.6 million by T-GmbH was then stopped by the reporting credit institution and submitted to the FIU as a STR in accordance with Section 46 (1) Anti-Money Laundering Act (AMLA).

26 The case study presented is a real case from the FIU's practice.

FIU Analysis and Dissemination

The FIU's analyses revealed that S-GmbH had also been reported by another credit institution due to conspicuous increases in turnover. S-GmbH had also applied for and received Covid-19 emergency aid. The managing director of T-GmbH had already been involved in a STR and accused in money laundering proceedings, which had been discontinued, but about which information had been provided to the tax authorities. In the present case, the reports were combined into an analysis report on Covid-19 emergency aid fraud and handed over to the competent State Office of Criminal Investigation (LKA).

The accused was convicted of subsidy fraud. The requirements for applying for emergency aid were not met, nor were the funds used for the intended purpose. The funds were used to pay off private loans and to purchase high-priced vehicles. Possibly the commercial transactions were only faked in order to convey the impression of legitimate business operation or other goods were traded. There were indications that the manager was only a straw woman, as there were connections to companies in the ownership of the clan milieu.

Implausible Business Activities

During the various forms of the lockdown in spring 2020, businesses in the retail and restaurant sector in particular were unable to continue their normal business operations. They either had to cease operations completely or were only allowed to continue in a modified form (e.g. exclusively pick-up/delivery service for catering businesses). Nevertheless, reporting entities were able to detect transactions on business accounts of the affected businesses that did not match the applicable pandemic-related prohibitions and restrictions. For

example, there were isolated reports of retailers who increasingly deposited cash in their accounts even though the business was closed. Furthermore, there were individual reports of catering businesses whose sales and related cash payments through the delivery service were significantly higher than the sales they had previously generated in the restaurant. Traders from other sectors also attracted attention due to implausible business activities.

Case Study – Protective Mask Sales²⁷

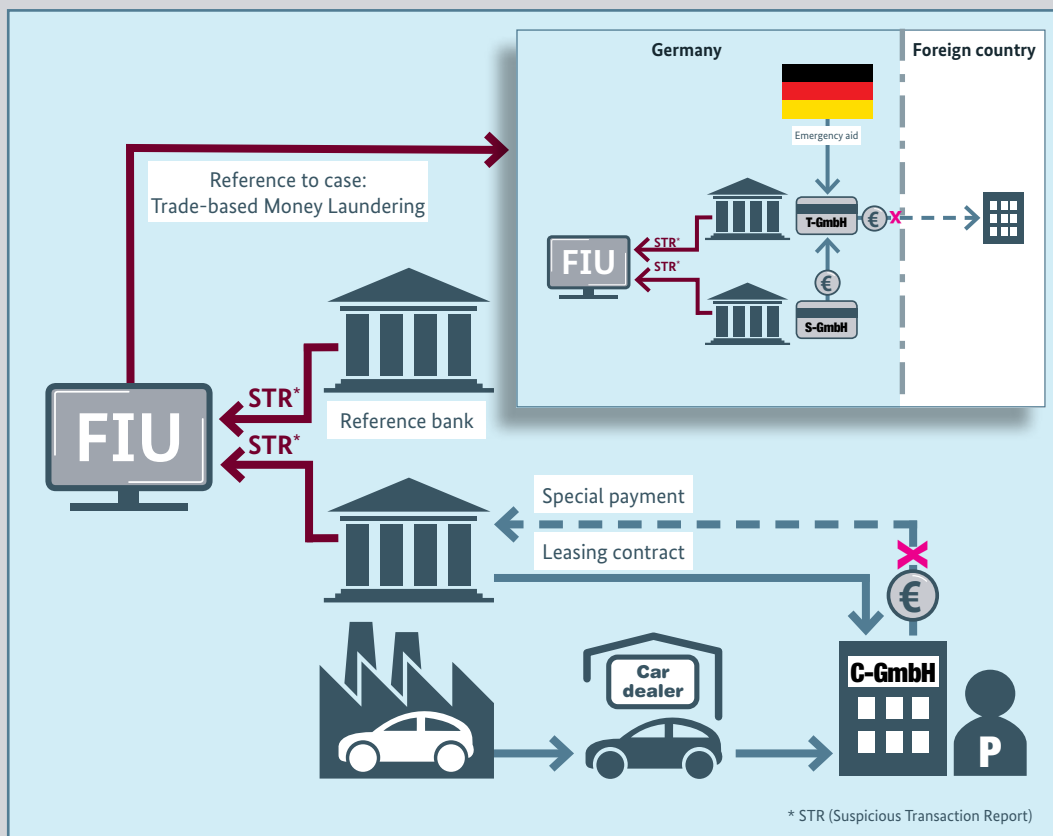


Figure 20: Case Study – Protective Mask Sales

Initial STR

The bank of a car manufacturer reported a commercial customer, C-GmbH. Within the framework of a leasing contract, the lessee wanted to make a special payment which, however, had not been contractually agreed and was therefore refused. The car dealer also had information that the individual P, the managing director of C-GmbH, had become conspicuous in connection with a transaction of S-GmbH. S-GmbH was involved in a case of fraud. During the examination of the economic circumstances, it was also noticeable that the reference bank stated in the application had also already submitted an STR because of C-GmbH. In this case, high cash receipts on the account had been identified, the origin of which could not be easily explained by the business model of C-GmbH. Allegedly, these cash receipts were related to the company’s entry into the protective gear business.

27 The case study presented is a real case from the FIU’s practice.

FIU Analysis and Dissemination

In the course of its analysis, the FIU was able to establish that there was another STR concerning C-GmbH. The reason for the report was the sudden increase in the turnover of C-GmbH in April 2020 due to the (alleged) business with protective masks, without it being comprehensible that the increase in turnover actually resulted from sales of protective masks. STRs were also received regarding the alleged purchaser of the protective masks in connection with the unclear origin of funds and cash transactions. The case was handed over to the competent State Office of Criminal Investigation (LKA).

Games of Chance

Due to the closure of casinos and betting offices during the lockdown and the temporary cessation of match operations in almost all sports, the volume of reports submitted by gambling organisers and brokers regarding terrestrial gambling (gambling at stationary locations, such as casinos) decreased significantly. At most, only a few gaming establishments were found to have made cash deposits during the lockdown, which, due to the closure of the establishments, were suspected of originating not from gaming operations, but from activities outside the industry or criminal activities. Furthermore, it was observed that the trend towards online gambling increased strongly due to the closures and that the associated reports, which were predominantly submitted by credit institutions, multiplied during the Covid-19

pandemic. For example, the number of reports submitted by reporting entities with the reporting reason 'anomalies in connection with games of chance/betting' rose from just over 900 in 2019 to almost 2,700 reports in the year under review. The legal transitional phase until the planned entry into force of the State Treaty on Gambling on 1 July 2021, the aim of which is to permit online gambling under certain conditions, leads to the partial toleration of online gambling by individual federal states. For gambling participants, this toleration could lead to the actual illegality of online gambling being seen as less and less serious. At the same time, the reporting entities continue to comply with their legal obligation to report these cases, since participation in online gambling continues to be a punishable offence.

Terrorist Financing and other Crimes Relevant to State Security

The FIU's findings on the Covid-19 pandemic in connection with the financing of terrorism and extremist groups focused less on terrorist attacks or related plans rather than on the raising of financial resources and the radicalisation and recruitment of new members.

It could be observed that extremist groups increasingly used social media to place their topics accordingly. They asked for donations or called for people to support the groups through paid memberships. In addition to the classic bank transfer, alternatives were often offered as a payment method, such as the possibility of donating via a so-called crowdfunding platform. Islamist groups, for example, called for donations for crisis regions or tried to fraudulently obtain emergency state aid from pandemic relief funds.

In the field of right-wing extremism, there are findings that the pandemic situation was used to recruit new members willing to pay for individual groups and to solicit financial support.

The worldwide restriction in freedom of movement and travel due to the pandemic meant that it was hardly possible for extremist groups to transport generated funds in cash both nationally as well as across borders. This circumstance was one of the reasons for the increased use of alternative, electronic forms and platforms of payment.

The STRs, that are related to Covid-19 and suspected terrorist financing, indicate that extremist groups have used the gained funds to further establish or expand their respective organisations. Exemplary goals were to gain additional supporters or members, and to further disseminate their respective ideologies.

The findings were shared with the FIU's partner authorities both nationally and internationally.

Case Study - Acceptance of an Covid-19 Emergency Aid Payment by a so-called Reich Citizen ('Reichsbürger')²⁸

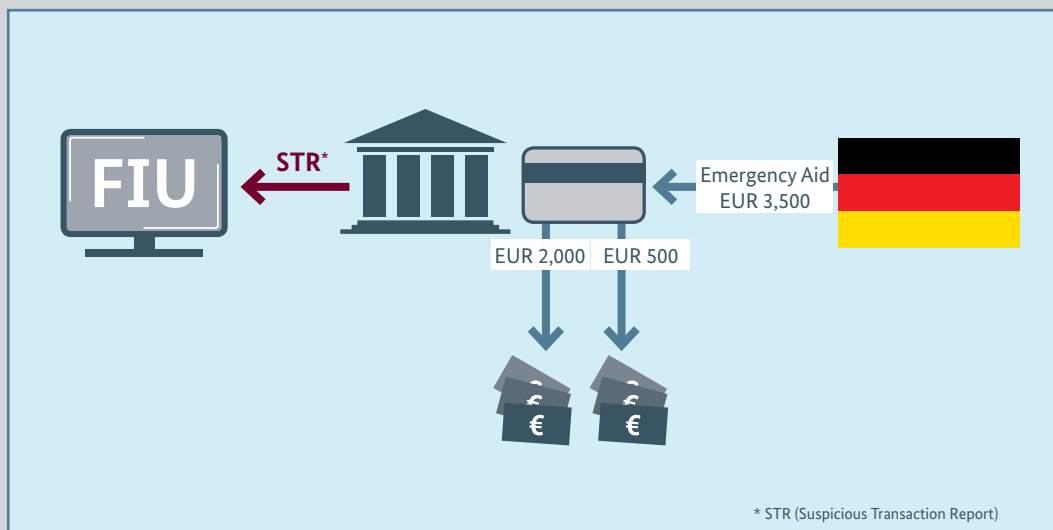


Figure 21: Case Study – Reich Citizen

Initial STR

The customer connection stood out due to the receipt of a Covid-19 emergency aid payment in the amount of EUR 3,500, from which a partial amount in cash was withdrawn the same day and another one a week later. The account of the reported person was kept as a garnishment protection account, regular wage payments were received on the account. A commercial activity related to the individual was neither known nor recognisable to the reporting entity. When the individual was asked whether he had maintained a registered business, he reacted indignantly and threatened to call in a lawyer. A business registration or similar proof of self-employment was not presented or provided.

FIU Analysis and Dissemination

In the course of the FIU analysis, it could not be ruled out that the Covid-19 emergency aid had been obtained without authorisation. The person was employed in a company as main occupation; the business registration provided later was only for a side-line business. Furthermore, it could be established that the individual had already appeared as a so-called 'Reich citizen'. A connection relevant to state protection or terrorism could therefore not be ruled out either. The analysis report with the aforementioned search results was subsequently handed over to the competent LEA.

28 The case study presented is a real case from the FIU's practice.

Case Study – Covid-19 Emergency Aid Fraud by Humanitarian Associations with Possible Links to the Salafist Scene²⁹

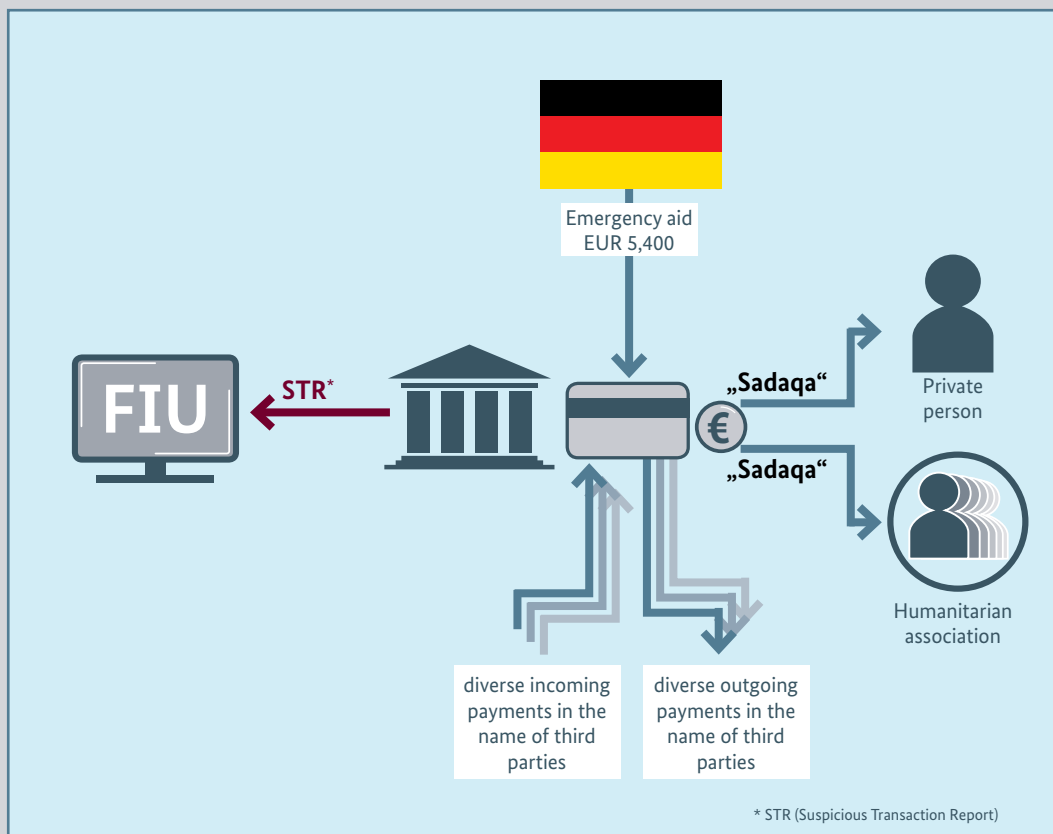


Figure 22: Case Study – Covid-19 Emergency Aid Fraud by Humanitarian Associations

Initial STR

The obliged entity reported a customer relationship that had attracted attention due to the connection to a public prosecutor’s investigation on suspicion of terrorist financing and due to an unusually large number of payments to or from several different accounts. The examination of the account transactions led to the finding that various incoming and outgoing payments were made in the name of third parties. Furthermore, a donation to a humanitarian association as well as a higher payment to a private individual were conspicuous, both of which were declared as Sadaqa (voluntary donation according to the Islamic faith). In addition, the receipt of a Covid-19 emergency aid in the amount of more than EUR 5,400 was determined, the receipt of which the reporting entity could not explain on the basis of the information available to it.

29 The case study presented is a real case from the FIU’s practice.

FIU Analysis and Dissemination

The operational analysis of the FIU confirmed that there were indications that the reported person could be acting as a financial intermediary for third parties. Within the scope of the analysis, the account transactions were analysed and various other investigations were included. With regard to the Covid-19 emergency aid received by the individual, the FIU was also able to establish the contradictory information and the associated assumption of possibly fraudulent receipt of the Covid-19 emergency aid. The person is said to have been the managing director of a construction company and at the same time to have appeared as self-employed on various platforms. The public social media profile of another individual, who appeared more frequently in the turnover, showed connections to the company of the person named in the STR. In addition, the profile of this third person showed references to Islamist sites and preachers. A connection with the financing of terrorism could therefore not be ruled out. The same applies to a possible subsidy fraud in connection with the payment of the Covid-19 emergency aid. The analysis report with the aforementioned search results was subsequently handed over to the competent LEA.

Outlook

The FIU assumes that the Covid-19 pandemic will have further effects on financial crime in the medium term. It is therefore imperative for the FIU, but also for all reporting entities and the national and international partner authorities of the FIU, to

continue to pay attention to unusual or suspicious activities of money laundering or terrorist financing in connection with Covid-19, to continuously update assessments and analyses and to continue the mutual exchange on a sustained basis.

Key Risk Area Trade-Based Money Laundering

TBML includes a money laundering process in which illicit funds are introduced into the legitimate economic cycle through the use of the international trading system and trade transactions in order to disguise the criminal origin of the funds.

TBML presents itself as multifaceted, adaptive and at times highly complex, which renders identification and prosecution difficult. In recent years, this form of money laundering has increasingly become the focus of anti-money laundering efforts. Alongside money laundering using the financial sector and money laundering using cash, it is considered one of the three main methods of money laundering used by organised criminal groups.

The Financial Action Task Force (FATF)³⁰ published a landmark study on TBML in 2006, identifying TBML as a widespread money laundering risk and outlining various techniques and *modi operandi* of TBML. This was followed by a best practice paper on TBML published by FATF in 2008, which provided authorities with impulses and suggestions in the fight against TBML. In 2012, the Asia Pacific Group on Money Laundering published another report that presented new developments in relation to TBML and obstacles in the fight against it.

Most recently, the FATF together with the Egmont Group published an updated report on TBML³¹ in December 2020, in which, among other things, current TBML techniques were identified.

The following represents common techniques of TBML, which in practice can also occur in combination and thus lead to increased complexity:

- **Over- or under-invoicing of goods and services:** In a trade transaction, the price of the goods or services is misrepresented in order to transfer incriminated value.
- **Over- or under-shipment of goods and services:** In a trade transaction, the quantity of the delivered goods or services is misrepresented, including ‘phantom shipment’, where no product is at all.
- **Falsely described goods and services:** In a trade transaction, the quality or type of goods or services is misrepresented, for example, low-value goods are declared as high-priced items to justify the transfer of higher amounts.
- **Multiple invoicing of goods and services:** Existing documentation is reused to justify multiple payments for the same shipment of goods, often involving different financial institutions, which makes it difficult to identify the money laundering offence.
- **Third-party intermediaries facilitating invoice settlement:** Unlike the TBML techniques described above, where both trading partners are complicitly involved in the money laundering scheme, this technique involves the misuse of legitimate trading partner for money laundering purposes. Thus, the settlement of the invoice of a legitimate trade transaction is being made by a previously uninvolved third-party unknown to the seller. In many cases, these third-parties are persons or companies whose country of origin or domicile differs from the country of the buyer. Often, accounts are at banks used which in turn are located in other countries.

³⁰ For information on FAFT, see the explanations in the section ‘International Cooperation’.

³¹ Cf. FATF – Egmont Group (2020), Trade-Based Money Laundering: Trends and Developments, www.fatf-gafi.org/publications/methodandtrends/documents/trade-based-money-laundering-trends-and-developments.html

- **Illicit cash integration:** In addition, the recent TBML-report describes various other, in part more complex techniques of TBML, including the so-called Offsetting Scheme (compensations taking place between different organised criminal groups or professional money laundering networks), so-called Surrogate Shopping Networks (individuals or networks purchasing high-value goods ostensibly on their own account, but in fact on behalf of their customers, and subsequently transporting the high-value goods abroad) or the infiltration of legitimate supply chains.

TBML can occur internationally in almost any trade sector. It cannot be pinpointed to any specific products. However, goods with wide pricing margins, extended trade cycles (e.g. shipping across multiple jurisdictions) and that are difficult for customs authorities to examine may be at higher risk.

Organised criminal groups or professional money laundering networks are often observed to be involved in TBML activities. The latter are networks that offer professional money laundering service in exchange for a fee. In doing so, such groups or networks may build up high levels of expertise in trade related fields and carry out complex trade transactions across different jurisdictions.

As noted in the NRA from 2018/2019, TBML is of significance for Germany as a business location due to the trade volumes generated here and the international nature of trade. Generally speaking, the international nature of trade poses a particular risk in terms of money laundering. For instance, the cross-border involvement of different actors can lead to unintentional practical or legal obstacles, which may hinder cross-border cooperation and the flow of information between companies, institutions and authorities involved. This can lead to challenges for identifying instances of money laundering and for subsequently prosecuting the perpetrators. In addition, the complexity and flexibility of the various, constantly evolving forms of techniques and modus operandi, which can also be found cumulatively, also add complexity to the identification and prosecution of TBML offences. For this reason, it is important to further raise awareness among the stakeholders from various sectors concerned.

As project lead to a project³² of the Egmont Group³³, the FIU was actively involved in the joint work of FATF and Egmont Group on TBML. The project collected and analysed insights and findings on TBML from participating FIUs and provided these, among other things, as inputs to the joint FATF and Egmont Group report on TBML.

³² For further information on the above-mentioned cooperation project, see the comments in the section 'International Cooperation'.

³³ For more information on the Egmont Group, see the section on 'International Cooperation'.

Modus Operandi – Over-Invoicing of Goods³⁴

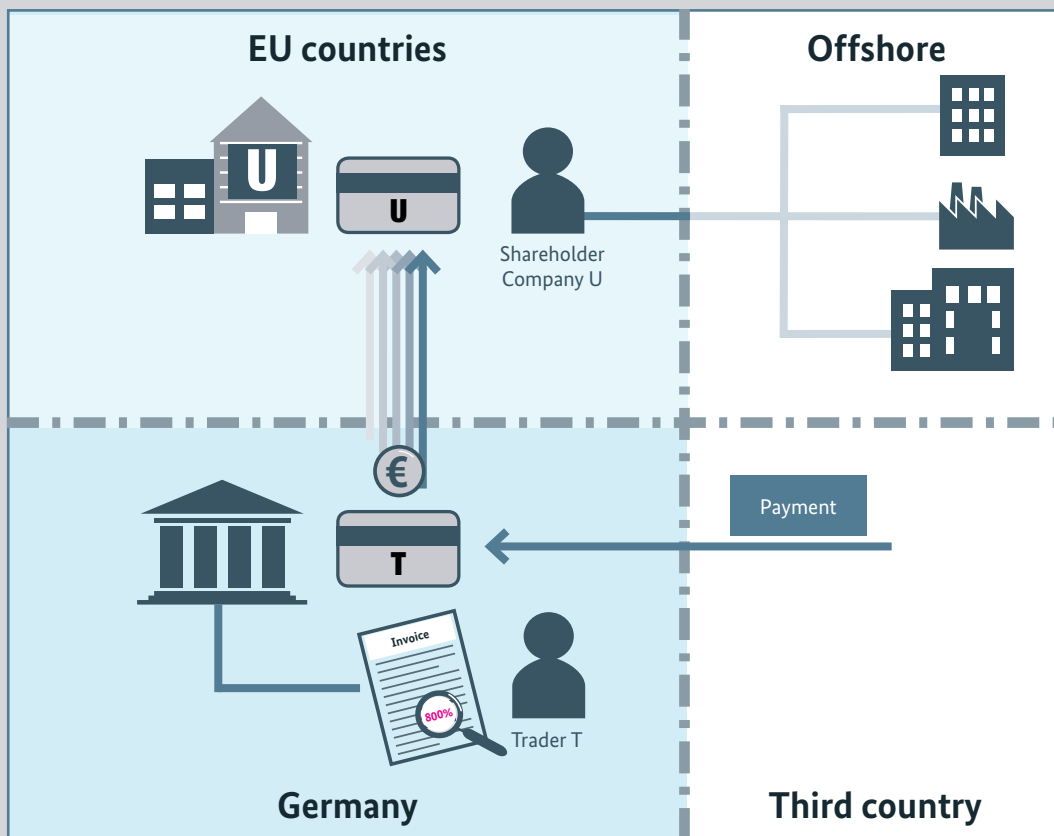


Figure 23: Modus Operandi – Over-Invoicing of Goods

A financial institution noticed suspicious transactions on the customer account of trader T: payments coming from a third country were received on this account, which were subsequently transferred in smaller tranches to company U, registered in another EU country. An internet search on the shareholder of company U revealed different conspicuous features, relating to his person to a number of directly and indirectly affiliated companies. For one of the payments Mr. T submitted an invoice to the reporting entity as proof of payment. According to the invoice, the payment was for the sale of 2.5 tonnes of grain for a total amount of approximately EUR 300,000. The invoice showed a price of approximately EUR 120 per kilo. Research showed that the market price for this sort of grain was in fact actually EUR 100 to 150 per ton, i.e. the in-invoice overstated the price by at least 800 times.

34 The modus operandi presented is based on an observable procedure from FIU practice.

Modus Operandi – Third-Party Intermediaries Facilitating Invoice Settlement³⁵

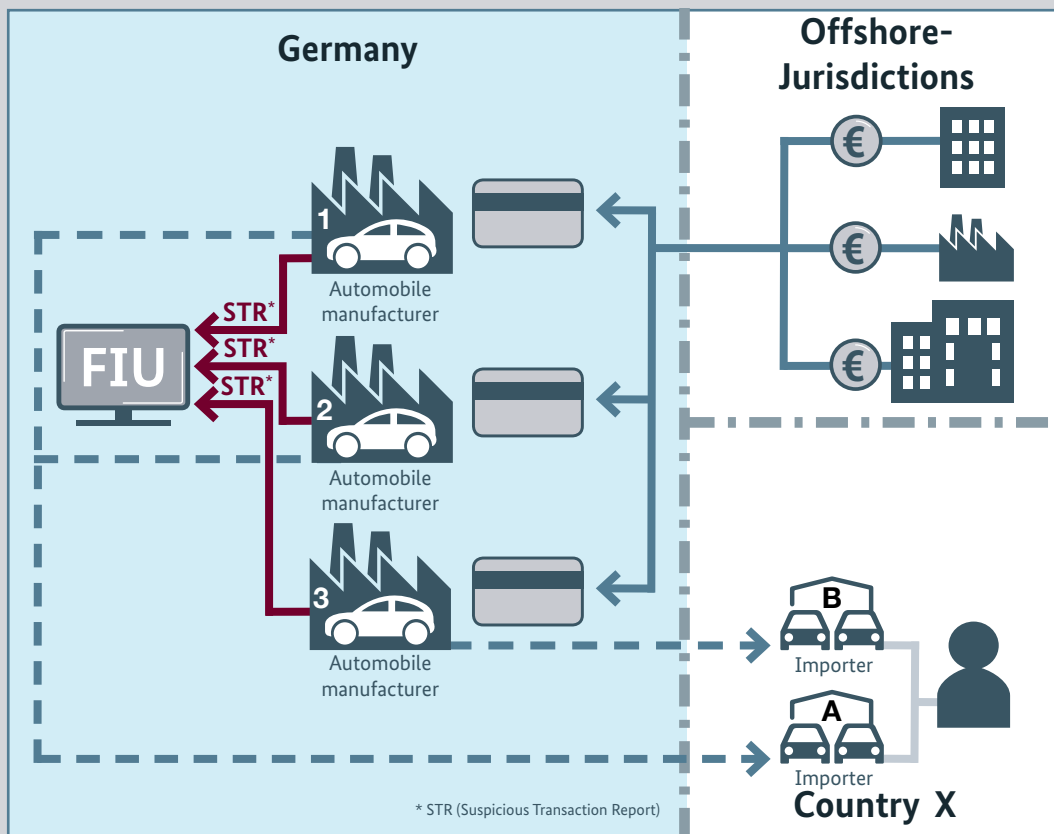


Figure 24: Modus Operandi – Third-Party Intermediaries Facilitating Invoice Settlement

A car manufacturer (1) reported to the FIU that a number of payments on behalf of his sales partner company A located in country X were made by various third-party payers. The third-party payers, which were registered in various jurisdictions, were all unknown to the car manufacturer.

Relating to company A, a second car manufacturer (2) working with this sales partner in country X also identified payments coming from unknown third-parties. Some of the third-parties were the same ones sending funds to car manufacturer (1). In some of the transactions, payment information mention the name of the car manufacturer (1), even though the funds were actually being sent to the car manufacturer (2).

In addition, a third car manufacturer (3) identified and reported third-party payments for his sales partner company B located in the same country X. Analysis revealed that the two sales partners A and B actually shared the same beneficial owner, a national of country X. One of the third party entities involved had been noted as a 'core company' of one of the so-called 'Laundromats'.

35 The modus operandi presented is based on an observable procedure from FIU practice.

Key Risk Area Commercial Fraud

The key risk area on commercial fraud and identity theft was revised in May 2020 with the participation of the LEA and the previous additional criterion of identity theft was deleted without substitution. The aim was to record all relevant cases of commercial fraud directly through the correspondingly expanded, associated risk focus 'Commercial fraud'. STRs that contained indications of commercial fraud, but not identity theft, were previously classified as 'other valuable facts' and processed as such.

Fraud

The term fraud stands for the deliberate deception of the victim by a perpetrator, in which a pecuniary loss is effectuated by a fallacy thus induced. Fraud is considered to be 'commercial' if the perpetrator intends to obtain a continuous source of income of some scale and duration by repeatedly committing the offence.

Identity theft

Identity theft is the misuse of personal data and login credentials by third parties. Personal data is used for criminal purposes or to discredit the victim.

A random detailed examination of those cases that involved commercial fraud shows that the method of commercial fraud was not necessarily accompanied by a misuse of identity by a third party, but that the fraudulent acts in question were also carried out using classic pass-through and financial intermediary accounts, without personal data having been misused by the perpetrators. In this case, persons were instated both knowingly and unknowingly as financial intermediaries.

The expansion of the risk focus described above ensures that the STRs received by the FIU that are related to commercial fraud without the additional criterion of identity theft are already prioritised within the scope of the expanded key risk area.

Financial Intermediary

The financial intermediary provides his own account to promptly transfer sums of money received through third parties to other accounts, mostly abroad. Part of the money may be retained as commission. Account holders are often unknowingly abused as financial agents. The methods are manifold and range from allegedly erroneously transferred amounts to pretending to be employed to establishing intimate contacts, e.g. in the context of a partner search.

Case Study – Commercial Fraud³⁶

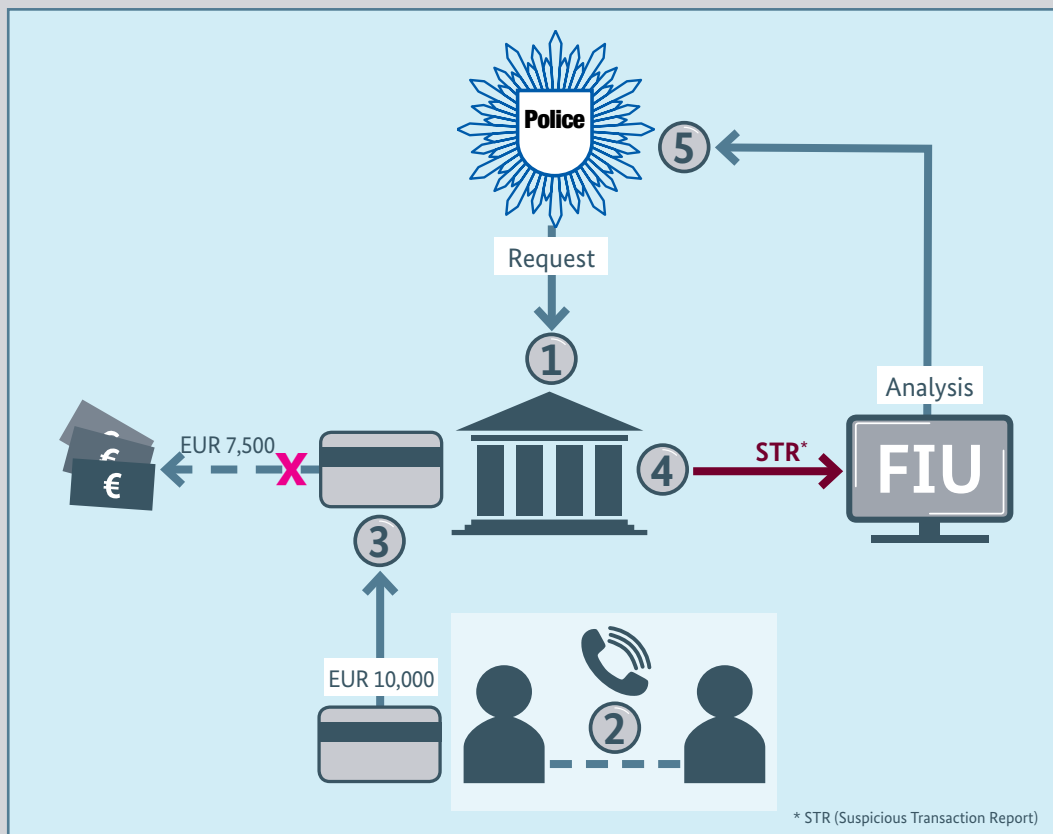


Figure 25: Case Study – Commercial Fraud

Initial STR

At the end of 2020, a reporting entity in the financial sector reported a suspected fraud by means of a STR pursuant to Section 46 (1) AMLA on the basis of an official request for information from a police inspection (1). The alleged victim had stated that a caller had pretended to be a police officer (2) and had explained that an arrest warrant had been issued against her, which could only be averted by paying a sum of about EUR 10,000. The allegedly injured party then transferred the demanded amount to the account held with the reporting entity (3). Based on the information available to her, the reporting entity could not rule out the possibility that her client had made his account available for the execution of fraudulent acts. After the customer intended to withdraw EUR 7,500 in cash from his account, the reporting entity reported the imminent transaction pursuant to Section 46 (1) AMLA (4) and thus suspended the execution of the transaction.

FIU Analysis and Dissemination

The day after receiving the report, the FIU immediately sent its analysis to the competent LEA (5), which then ordered the amount of EUR 7,500 to be seized.

36 The case study presented is a real case from the FIU's practice.

As the development of case numbers in the course of 2020 shows, the number of related case analyses in the context of the risk focus on commercial fraud initially remained at a constant level. The significant drop in June can be explained by the

pandemic. Although a significant number of STRs were submitted to the FIU in June, which were directly related to the Covid-19 emergency aid payments and required prioritised processing, they were not assigned to the key risk area listed here.³⁷

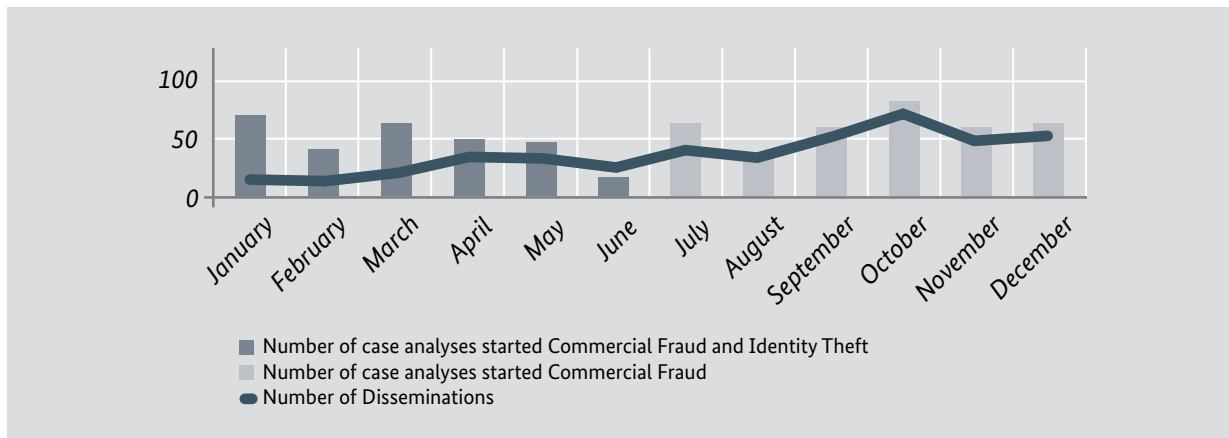


Figure 26: Development of the Number of Case Analyses with reference to Key Risk Area Commercial Fraud (and Identity Theft)

While the number of case analyses started showed only a slight upward trend over the course of the year, the rate of disseminated cases rose considerably in the second half of the year. One of the reasons for this is that the number of incoming requests from national partner authorities in connection with commercial fraud increased over the course of the year and the associated analyses subsequently led to a dissemination to the competent LEA in most cases. In the FIU’s view, this is an indication that the LEA are increasingly making use of their possibility to request the information

available at the FIU and to incorporate it into their criminal investigations. The development of the figures shows that the average number of disseminations rose from about 20 disseminations per month in the first half of the year to an average of about 50 disseminations per month in the second half of the year.

The FIU takes comprehensive account of the development of crime by aligning its key risk areas accordingly – in this case with regard to fraud crime.

37 See the explanations above on ‘Special topic Covid-19’. Since STRs in connection with Covid-19 could not originally be assigned to a key risk area, the FIU formed its own focus of work. In this way, the corresponding STRs could be transmitted directly to the LEA.

Identity Theft

Although the key risk area is now oriented towards commercial fraud in general due to the abandonment of the additional criterion 'identity theft', the misuse of personal data remains a common modus operandi of money laundering.

Direct banks in particular offer customers the option of having their identity and legitimation checked by means of a video identification procedure when opening an account. In such video identification procedures, the identity check that the financial institution has to carry out when opening an account is carried out by means of a video conference. The customer has to identify himself during the video conference and answer questions related to his identity and legitimation. This means that customers do not have to visit a branch in person or take part in a Post-Ident procedure to prove their identity. The Video-Ident procedure offers a considerable potential for abuse. For example, personal data is requested through 'social engineering' in the context of allegedly conducting job interviews, setting up rental deposit accounts or allegedly testing video ID procedures and then misused to open further accounts. The perpetrators then use the accounts opened under the name of their victims for criminal purposes, mostly in connection with commercial fraud (e.g. for operating fake shops) or directly for money laundering.

In 2020, the FIU was able to determine that the reporting entities increasingly reported accounts held in Germany by persons residing in other European countries. The transaction behaviour often indicated that the funds originated from commercial fraud (e.g. phishing, merchandise fraud/fake shops, love scamming, etc.).

Phishing

Phishing is the obtaining of passwords and other personal information with fake e-mails or websites. With the 'fished' personal data, fraudsters can conduct almost any business on the Internet in the name of the injured party.

In these cases, the account balance was used for cash withdrawals at ATMs in European and non-European countries or for immediate forwarding to foreign accounts or payment service providers. In this context, it was also noticeable that in many cases, higher-value credits were immediately forwarded in various, smaller amounts to different accounts at home and abroad.

The FIU's role as a central agency makes it possible to establish links between STRs that differ in location and time and the persons and accounts involved. Through direct transmission to German LEA and European FIUs, it was possible to secure large account balances. Only by meticulously analysing the account transactions and through consistent international cooperation it is possible to track down the perpetrators acting in the background.

Case Study – Identity Theft³⁸

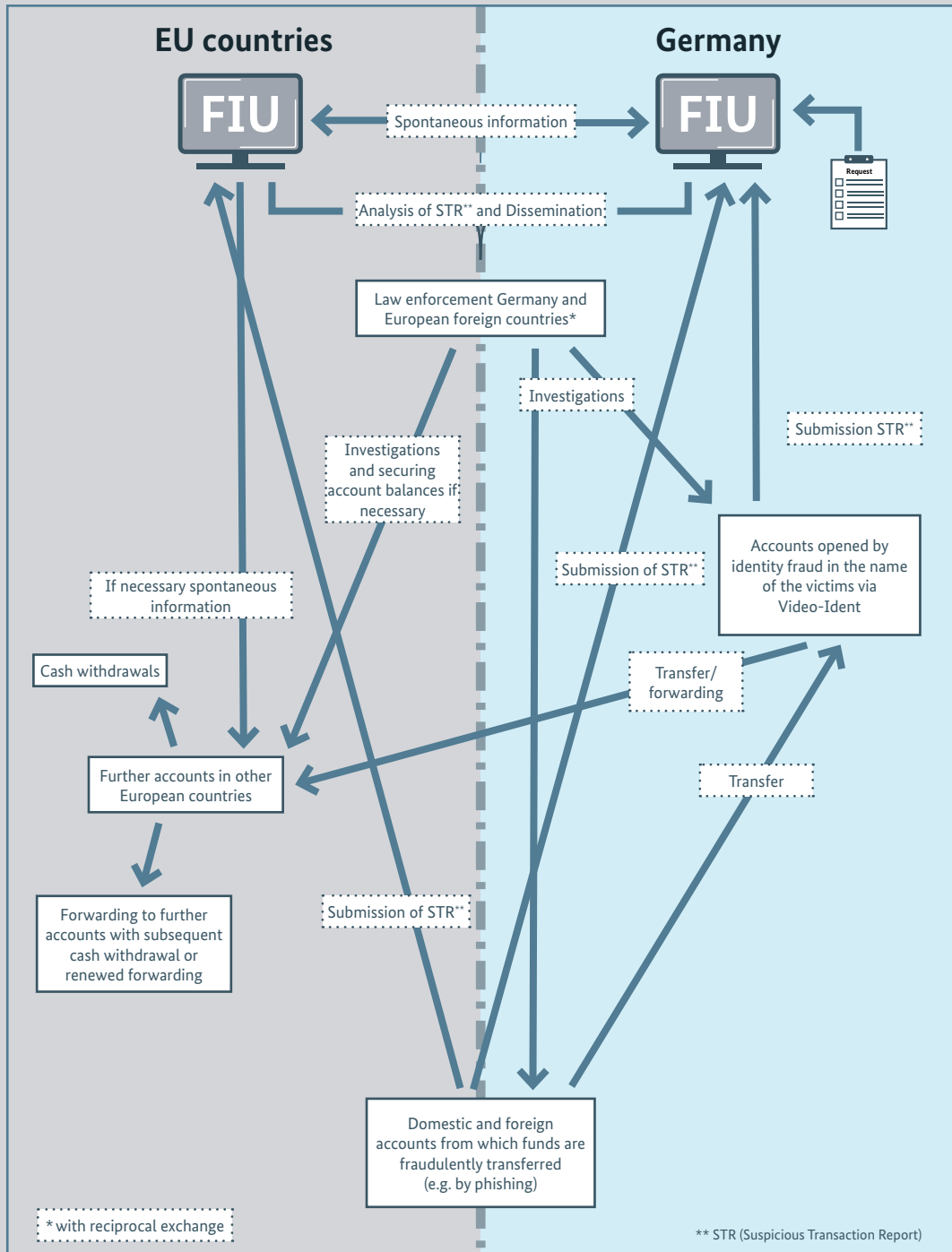


Figure 27: Case Study – Identity Theft

38 The case study presented is a real case from the FIU's practice.

Initial STR

In the context of an urgent request for information from a German police department, a related STR was identified. The STR referred to a German account from which funds were transferred to ten foreign residents with accounts opened via video-identification at German banks. It was suspected that the accounts had been opened by means of phishing.

FIU Analysis and Dissemination

In the course of the analysis, it was discovered that other banks had also submitted STRs for the ten beneficiary accounts, which indicated possible identity abuse, and that the credits on all ten beneficiary accounts were immediately forwarded to an account in another European country belonging to a person resident in Germany.

The FIU immediately forwarded the results of the analysis to various German LEA. In addition, the police department that had made the urgent request for information was notified directly. Furthermore, the facts of the case were forwarded to the corresponding FIU in another European country.

The FIU Germany received information from the FIU concerned that a five-digit account balance could be secured. However, some funds had already been disposed of in cash or transferred to other accounts.

Key Risk Area Use of New Payment Methods

The FIU has strengthened its risk-based approach with the application of key risk areas also in the area of new payment methods in 2020. Against the backdrop of the continuous development of payment methods and related processing platforms as well as the increasing number of new providers,

the FIU continuously assesses the risks arising from these developments with regard to money laundering and terrorist financing and validates its key risk areas on the basis of corresponding findings.

Virtual Assets

After the annual reports of the previous years had already dealt in depth with the topic of virtual assets, these were also a focus of activities in 2020 within the framework of the key risk area ‘use of new payment methods’.

With the entry into force of the German Act Implementing the Amending Directive to the Fourth EU Money Laundering Directive on 1 January 2020³⁹, the virtual crypto custody business was legally anchored as a financial service and the classification of virtual assets as financial instruments. This is accompanied by a licensing requirement for companies that want to provide services in this context. In this regard, transitional provisions existed until 30 November 2020. Irrespective of the transitional provisions, corresponding companies have been obligated parties within the meaning of the AMLA since the law came into force.

So far, the FIU has not seen any significant effects from the changed legal framework. By the end of 2020, only a few companies beyond the

already known providers can be identified that offer crypto custody business or other banking/financial services in connection with virtual assets, have registered as reporting entities and have already submitted suspicious transaction reports. An increase is to be expected if further companies are granted permission by BaFin, in particular for the provision of crypto custody business.

Compared to 2019, the number STRs in which the reason for reporting was ‘anomalies in connection with virtual currencies’ more than doubled. In total, around 2,050 STRs had this reason for reporting (2019: around 760). The number of reports in connection with virtual assets has thus increased disproportionately compared to the total number of reports. An increasing trend was also evident in the course of the reporting year.

³⁹ Act on the Implementation of the Fourth EU Anti-Money Laundering Directive, the EU Funds Transfer Regulation and on the Reorganisation of the Financial Intelligence Unit of 23 June 2017 (Federal Law Gazette I, p. 1822); Act on the Implementation of the Amendment Directive to the Fourth EU Money Laundering Directive of 12 December 2019 (Federal Law Gazette I, p. 2602).

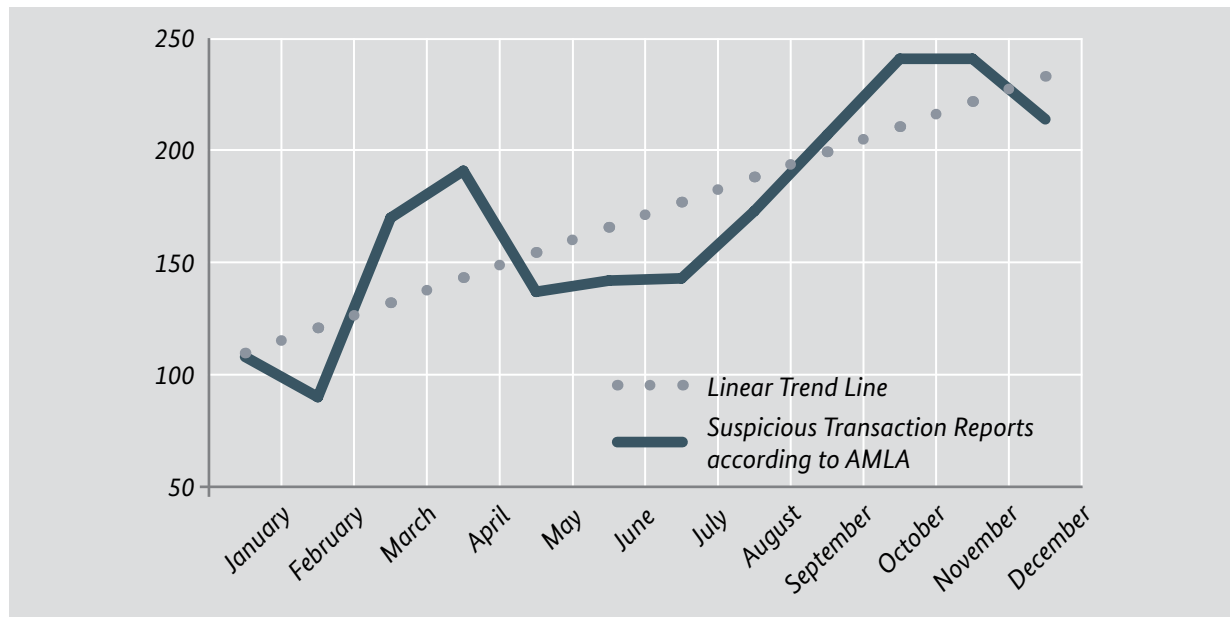


Figure 28: Suspicious Transaction Reports with the Reporting Reason ‘Anomalies in Connection with Virtual Currencies’

As in the previous year, a large part of the STRs are related to fraud offences. The victims are usually persons whose orders for goods (via auction portals, classified ad websites or fake shops) came to nothing, who were tricked into fake investments or where the perpetrators gained control over bank accounts (e.g. through phishing). In 2020, there were also numerous STRs relating to Covid-19 emergency aid. The method of practice is always similar: For the payment of the purchase prices, accounts are used which the perpetrators have directly or indirectly at their disposal. From there, the funds are transferred directly, either to (often foreign-based) trading centres for virtual assets or first to other accounts with subsequent conversion into virtual assets.

As before, the STRs come almost exclusively from credit institutions (more than 96%). Reporting entities often conclude that their customer could be acting on behalf of third parties, e.g. due to transaction patterns that indicate a mere transfer of funds, and therefore assume a financial intermediary activity, which is reported accordingly. From the facts contained in the STRs, it can also be seen that injured parties had often already reported the fraud to the police or contacted the account-holding institutions, which then submitted STRs. Compared to 2019, STRs were also filed more frequently for direct transactions in virtual currencies, e.g. if a customer’s virtual assets were connected to so-called mixers⁴⁰, computer fraud, extortion or wallet providers with a high degree of anonymity⁴¹, or if transactions were related to darknet marketplaces.

40 Mixers (or tumblers) are service providers that enable the mixing of incoming and outgoing funds in crypto assets of any origin, including criminal origin, and thus make it difficult to trace transactions and identify the wallet addresses of the sender and recipient of the funds.

41 These are providers of wallets with extended anonymisation properties, e.g. through the use of ‘CoinJoin’ transactions, which restricts or makes it difficult to clearly trace the origin and destination of the transaction.

Darknet Marketplaces

Darknet marketplaces are certain virtual marketplaces or shops for trading in often illegal goods and services of all kinds. These are set up in the so-called darknet, a hidden part of the internet that is only accessible via a certain browser. Payment is usually made by means of virtual assets.

In December 2020, the FIU first published a typologies paper on transactions involving virtual assets and crypto custody businesses, which provides information on how to detect misuse for money laundering or terrorist financing in this context. Since conspicuous behaviour is not limited to transactions in virtual assets, but also the interaction with FIAT currencies, such as the euro or US dollar, must be considered, the paper is addressed to all reporting entities. The FIU thus takes into account the special importance of the topic on a global level.⁴²

Case Study – Suspicious Account and Transaction Network⁴³

Initial STR

In several STRs, a credit institution reported various suspicious accounts opened online by persons from Northern Europe since the beginning of 2020, which showed a similar, suspicious transaction pattern. Funds received from payment service providers abroad, predominantly in the five-digit range, were promptly forwarded to virtual asset trading venues and other persons. For example, person A received a total of EUR 100,000 from payment service assets provider A in several transfers and promptly transferred this amount to person B, payment service provider B and virtual asset exchange B in total. Person B received EUR 150,000 from payment service provider A as well as EUR 40,000 from person C. Person B forwarded the EUR 150,000 received directly to person D, who then transferred EUR 200,000 to virtual assets exchange C. The EUR 40,000 received from payment service provider B were transferred to virtual assets exchange C in a timely manner. The EUR 40,000 that person B received from person C came from incoming transfers from accounts at payment service provider A and virtual assets exchange A for EUR 20,000 each.

42 See the conclusions and recommendations of the '4th Global Conference on Criminal Finances and Cryptocurrencies' of 18/19 November 2020, available at: https://www.europol.europa.eu/sites/default/files/documents/recommendations_-_4th_global_conference_on_criminal_finances_and_cryptocurrencies.pdf

43 The following is a simplified excerpt from a larger case complex that the FIU was able to uncover. The amounts mentioned in the chart are exemplary and are intended to illustrate money flows within the network.

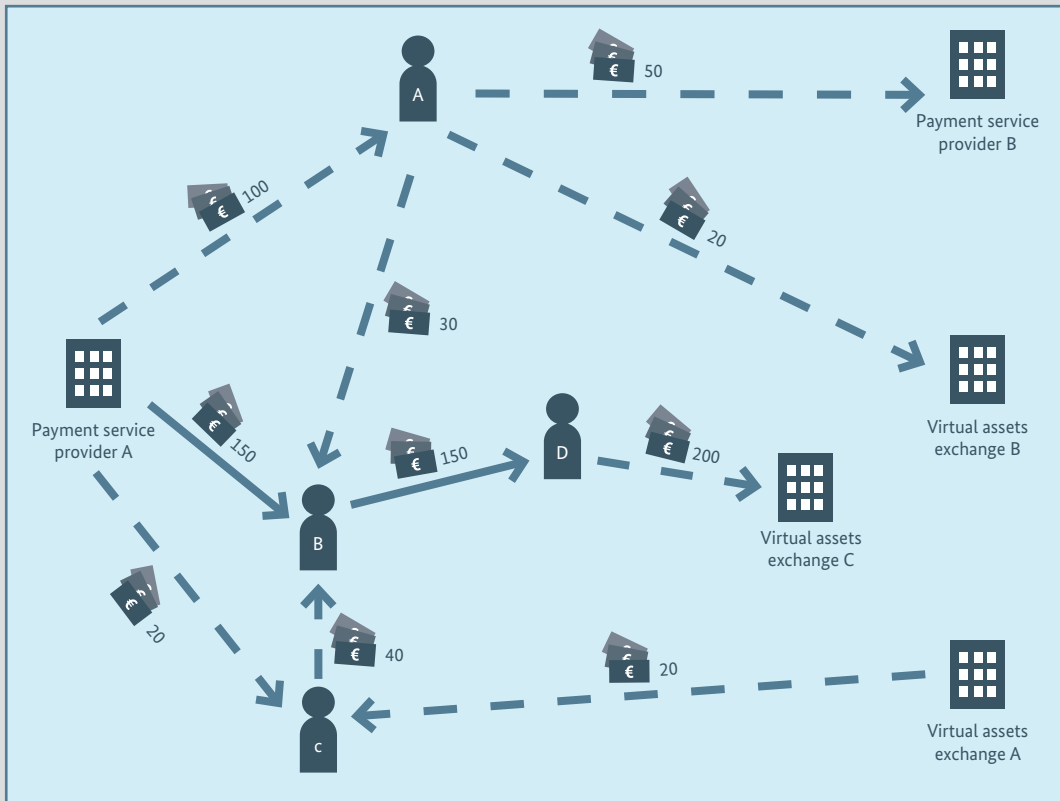


Figure 29: Case study – Suspicious Account and Transaction Network

FIU Analysis and Dissemination

The FIU’s analyses revealed a complex network of more than 30 accounts through which incoming funds were collected and transferred, even among themselves and without any apparent economic reason, before leaving the network and being forwarded to foreign virtual assets exchanges or payment service providers. The size and complexity of the network indicated professional structures in the background that coordinated the money flows within the system, especially since the inflows and outflows were almost balanced throughout the system under consideration. Since no German citizens or persons residing in Germany were involved in the network, FIU Germany informed several affected partner FIUs in Northern Europe about the findings and the persons involved.

Case Study – Money Laundering of Fraudulently Obtained Covid-19 Emergency Aid⁴⁴

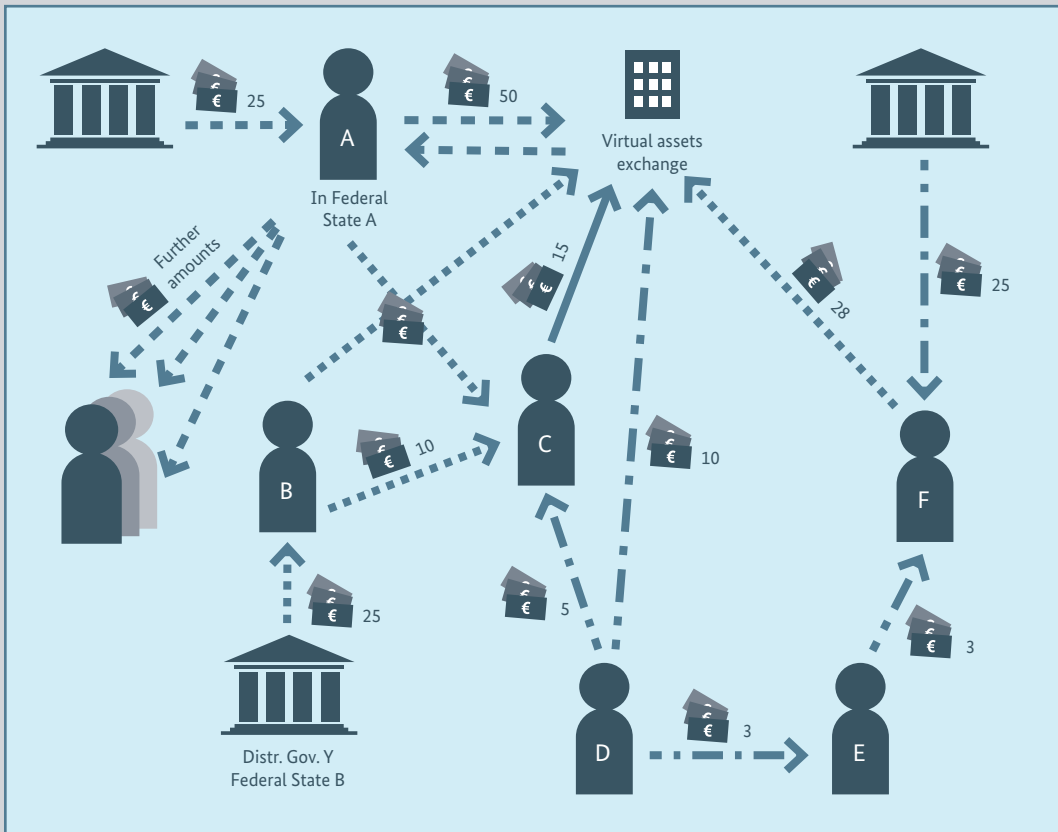


Figure 30: Case Study – Money Laundering of Fraudulently Obtained Covid-19 Emergency Aid

Initial STR

The starting point for the exposure of this case complex was the report of a bank, which noticed the receipt of a large amount of Covid-19 emergency aid with a different recipient name on the account of its client (person A), who was self-employed. The credit was conspicuous because the client was resident in the federal state of A, but the emergency aid was paid by the federal state of B. Another factor was the fact that the client was a self-employed person. Another clue was that the client transferred the funds received to a virtual assets exchange and several private individuals on the same day. The funds transferred to the virtual assets exchange arrived a few days later in the account of the client, who forwarded them to third parties.

⁴⁴ The case example shown is a real case from FIU practice, which has been simplified and made anonymous for reasons of clarity. The amounts mentioned in the chart are exemplary and are meant to illustrate money flows within the network.

FIU Analysis and Dissemination

The FIU’s analyses revealed that one of these private individuals (person C) was also the subject of a STR. This person became conspicuous through the receipt of large sums of money from unknown persons, which were promptly forwarded to virtual assets exchanges and other persons.

On the basis of a transaction analysis, several financial intermediaries could be identified who contributed to the concealment of funds from criminal activities (here, among other things, fraud) by splitting and transferring them to other persons and virtual assets exchanges. The STRs revealed that some of the financial intermediaries were victims of a so-called job scam.⁴⁵ The FIU forwarded the reports and findings to the respective competent LEA.

Findings and Developments Outside the Field of Virtual Assets

In order to identify developments within the key risk area of the use of new payment methods that go beyond the topic of virtual assets, a special evaluation of STRs from the year 2020 was carried out. All reports that were received by the FIU in the reporting year were considered and assigned

to the key risk area ‘use of new payment methods’, but without those STRs that were submitted with the reporting reason ‘anomalies in connection with virtual currencies’. In total, this applies to almost 2,900 reports.

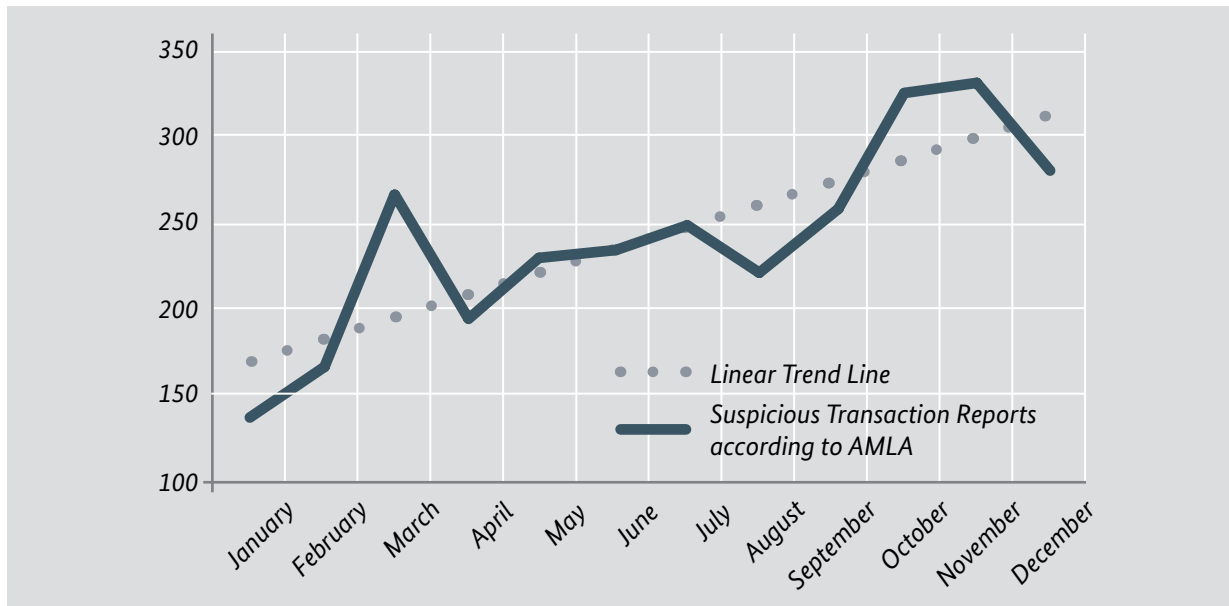


Figure 31: Further Reports in the Key Risk Area ‘Use of New Payment Methods’

⁴⁵ Job scams are, among other things, dubious job offers that serve to obtain personal data and bank details. A possible modus operandi in this context is that the often gullible victim is employed, for example, as a ‘financial manager’ and the task consists of transferring money received on their own account to other account connections in return for remuneration or withdrawing cash and depositing it elsewhere.

With regard to the number of incoming STRs considered here, there was also a clear upward trend in the course of 2020. The majority of reports were submitted by credit institutions, with only just under 1% of reports being submitted by financial service institutions.

A large proportion of the reports refer to virtual assets. Nevertheless, *modi operandi* can also be observed by means of new payment methods – especially peer-to-peer solutions⁴⁶ or mobile payment procedures (e.g. Apple Pay, Google Pay) as opposed to classic bank transfers, direct debits or credit card payments. Peer-to-peer solutions or mobile payment methods seem to be particularly suitable for such activities, as they offer not only the advantage of convenient use through e.g. intuitive user interfaces and location-independent access to user accounts, but also fast account opening and legitimation via the internet, as well as the fast execution of transactions without the usual execution times for bank transfers. An evaluation shows that at least 35% of the STRs relate to comparatively young companies with a focus on peer-to-peer solutions or mobile payment methods.

There was a noticeable increase in the number of STRs in which the reporting entities suspected a fraudulent background with previous identity abuse or an abusive activity of the account holder as a financial intermediary, whereby the accounts mostly had the characteristics of a so-called

pass-through account, in which funds from different clients were received and then promptly flowed out again, often to virtual exchanges. In many other cases, the origin of the funds was unclear in connection with peer-to-peer transactions or the loading of e-wallets, or it was apparently winnings from games of chance, which in turn were often forwarded to trading centres for virtual assets.

Reporting entities in the context of mobile payment methods or peer-to-peer transactions are often the banks cooperating with the respective providers.

Within the scope of the analysis of an individual case (see also the next case study), it became apparent that, according to the information contained in the STRs, when using a peer-to-peer payment method, amounts were deliberately transferred that were below the threshold amount for a required TAN entry. In this way, the transaction speed can be increased on the one hand, and on the other hand, hijacked accesses can be used more easily.

Based on the analysed STRs from the key risk area ‘Use of new payment methods’, other payment methods, such as payment by voucher cards and ‘cash-to-code transfers’⁴⁷, have only been of minor importance so far. Any developments will continue to be monitored.

46 Peer-to-peer solutions here refer in particular to payment methods where money can be transferred directly to contacts via smartphone (e.g. PayPal, Kwitt or Paydirekt).

47 With a cash-to-code transfer, a (cash) code generated during payment on the Internet is presented at a partner shop and the required amount is paid in cash there. In this way, either a credit balance can be created on an online credit account, e.g. for online games, or a purchase of goods can be paid for subsequently.

Case Study – Network with Financial Intermediaries⁴⁸

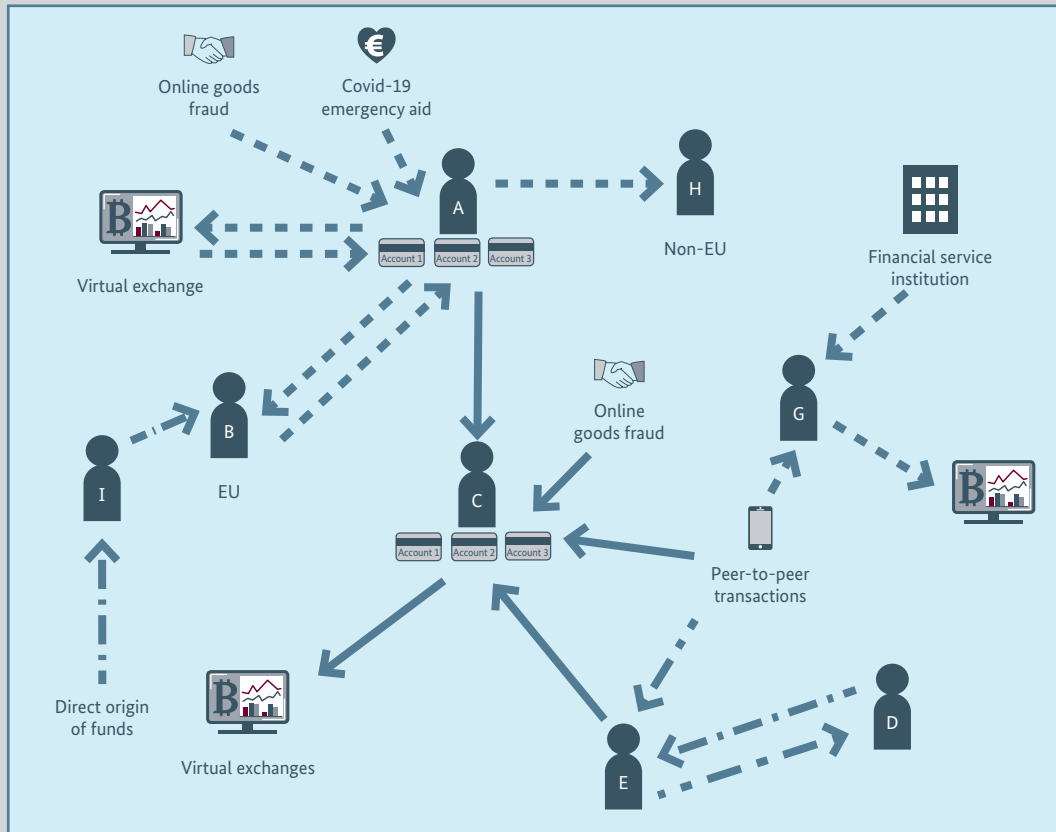


Figure 32: Case Study – Network with Financial Intermediaries

Initial STR

The starting point for this case were reports from various credit institutions about money received on customer accounts that were below the limit for TAN-required payments by means of mobile phone-to-mobile phone transfers and were forwarded promptly (exemplified in the figure by persons C and E). Some of the reports were based on transfer recalls with reference to fraud, among other things from illegally obtained online banking access. The purpose of the transfer often contained user names or indicated a reference to virtual assets.

FIU Analysis and Dissemination

The FIU’s analyses revealed a complex network of persons (e.g. persons A and C) with a large number of bank accounts. These persons received funds from various natural persons or legal entities. In addition to the mobile phone-to-mobile phone transactions below the TAN limit, this also involved larger sums from e.g. online goods fraud or Covid-19 emergency aid.

48 The following is a simplified excerpt of a larger case complex that the FIU was able to uncover. The flows of money shown in the diagram are exemplary and serve to illustrate the situation.

The funds received were transferred by the central actors (e.g. persons A and G) to virtual assets exchanges, financial service institutions and also to accounts of natural persons (e.g. person H). The assumption was that this was a professional network used by several actors. In this context, there was a large number of disseminations to various LEA.

This example shows, on the one hand, the importance of financial intermediaries (e.g. person E) as elementary building blocks for money laundering networks and, on the other hand, the increasing specialisation of actors in these activities, with which they offer services to other criminals, which becomes clear through the different money receipts (money from Covid-19 subsidy fraud, online goods fraud, etc.).

Key Risk Area Misuse of NGOs/NPOs

The risk focus on misuse of NGOs/NPOs in the area of terrorist financing, which was introduced within the framework of the FIU's RBA, also proved its worth in the past year. In the reporting year, approximately 870 reports were assigned to this area. Compared to the previous year, it is noticeable that the number of STRs related to the misuse of NGOs/NPOs has increased significantly.

A sectoral risk analysis carried out by the Federal Ministry of the Interior, Building and Community regarding terrorist financing through (the misuse of) NPOs shows comparable tendencies.⁴⁹ In the reporting year, the FIU forwarded to the competent authorities more than 300 analysis complexes, which can be assigned to the area of misuse of NGOs/NPOs.

Non-Governmental Organisations (NGOs)

Non-governmental organisations are private or public organisations that represent political interests but are not subordinate to the state or government and do not pursue a profit-making objective. In principle, this includes all associations or groups that represent common interests (e.g. in the areas of environment and animal protection, human rights protection, health care and development work). These include, for example, trade unions, churches and citizens' initiatives, but also foundations and associations.

Non-Profit Organisations (NPOs)

Non-profit organisations are organisations that operate on a non-profit basis and are founded for social (including religious, cultural, educational, social and family) purposes. They can be established either in private form, for example as an association, federation or foundation, or as public NPOs, for example as a public company or administration. Unlike NGOs, however, they are not fundamentally dedicated to political issues and also generate their own financial resources, i.e. they are not financed exclusively by membership fees.

⁴⁹ Cf. Sectoral Risk Analysis – Terrorist Financing through (the Misuse of) Non-Profit Organisations in Germany, Status 2020, Federal Ministry of the Interior, Building and Community, p. 7.

Characteristics of Terrorist Financing

Terrorist financing is characterised by the internationally recognised triad of ‘raising’, ‘moving’ and

‘using’. These typical characteristics are illustrated using the example of the misuse of NGOs/NPOs.

Raising:

In a first step, funds are raised or generated. Depending on whether an NPO/NGO is misused for terrorist financing or is founded specifically for this purpose, the generation of funds can have different characteristics. NPOs created specifically for the purpose of terrorist financing often call for donations outside of crisis areas. By presenting themselves as supposedly humanitarian organisations, NPOs generate their funds through both knowing and unknowing supporters, although the funds are later used in whole or in part for terrorist financing.

Moving:

The financial resources are then transferred with the aim of temporarily storing them until they are used or to conceal their actual purpose. To this end, private accounts are sometimes interposed to subsequently disburse the money in cash and smuggle it through cash couriers, for example. Alternative transaction methods such as ‘hawala-banking’ can also be used to disguise the terrorist use of the funds.

Hawala-Banking:

The so-called ‘hawala-banking’ (also: ‘hawallah’, from the Arabic ‘to transfer’ / ‘to change’) is an informal money transfer system. Synonymously, terms such as ‘Hundi’ (India), ‘Fei ch’ ein’ and ‘Chop Shop Banking’ (China) as well as ‘Poey Kuan’ and ‘Flying Money’ (Thailand) are also used here. The FATF therefore summarises the further typology of such trust-based and unregulated money transfer systems as ‘hawala and other similar service providers (HOSSPs)’. HOSSPs are defined as money transfer service providers that are linked to specific geographic regions or ethnic communities and arrange the transfer and receipt of money or its equivalent. Payments are settled in the long term through commercial transactions, cash and net settlements. Since the financial transactions take place outside the financial sector, the parties involved and/or economic backgrounds are often not or only to a limited extent comprehensible. Besides being used for legal purposes, informal payment systems are therefore vulnerable to being used for money laundering or terrorist financing.

Using:

Finally, funds are used directly or indirectly to finance terrorist organisations or attacks. However, due to the prior concealment of the use of

funds, it is usually difficult or impossible at this point to identify the connection of a transaction to terrorist financing.

One-to-many:

STRs in which incoming payments can be identified that are subsequently transferred to numerous recipients (mostly other private accounts or association accounts) without a plausible connection between the parties involved in the transaction being identifiable.

Many-to-one

STRs in which incoming payments can be identified that are debited to various ordering parties (mostly other private accounts or association accounts) without a plausible connection between the parties involved in the transaction being identifiable.

The transitions between the characteristics of terrorist financing are fluid. Reported facts can

therefore always concern several characteristics.

Findings on the Approach of Alleged Humanitarian Organisations in Acquiring Donations

Available findings show that supposedly humanitarian organisations in particular are used specifically to finance terrorism. The organisations give the impression of providing humanitarian support to people who are in acute need due to crises, conflicts or natural disasters and who are unable to cope with them on their own⁵⁰, and thus disguise their terrorist background. A common means of financing terrorist activities is so-called donation-based crowdfunding.⁵¹ In addition to the fundamentally legitimate form of generating funds, this represents a possibility of terrorist financing. In this case, persons or organisations aggressively solicit donations for ostensibly legal charitable purposes, the ultimate use of which, however, may correspond to the realisation of a terrorist offence. Crowdfunding makes it possible to reach a large number of potential supporters with little effort. Gullible donors are encouraged to donate through social media for a supposedly 'good cause', without possibly being aware of a possible misuse of their donations.

Behind such appeals are supposedly humanitarian organisations, which are often officially registered associations with a professionally designed website. This is supposed to convey a certain seriousness.

Compared to organisational forms such as foundations and non-profit limited liability companies, registered associations are generally considered to have a higher risk of abuse with regard to terrorist financing. The reasons for this are seen in the generally higher requirements for foundations and limited liability companies, for example with regard to regular accounting and the necessary share capital at the time of foundation. The foundation and management of associations are much less complicated with regard to these formalities⁵². In more than 50% of the above-mentioned approx. 870 STRs with reference to the key risk area 'Misuse of NGOs/NPOs', a connection with associations could be identified.

50 Cf. <https://www.auswaertiges-amt.de/de/aussenpolitik/themen/humanitaere-hilfe/huhi/205108>.

51 Cf. NRA 2018/2019, Federal Ministry of Finance, p. 101.

52 Cf. Sectoral Risk Analysis – Terrorist Financing through (the Misuse of) Non-Profit Organisations in Germany, Status 2020, Federal Ministry of the Interior, Building and Community, pp. 50 to 51.

Excursus Crowdfunding⁵³

Crowdfunding is a form of financing initiated with the aim of financing a specific project or undertaking with the support of the so-called crowd. Crowdfunding can be further differentiated both in terms of the actors involved and in terms of the possible forms, whereby mixed forms can also occur in practice. Furthermore, a fixed group of capital recipients can promote several projects in parallel, each of which is realised by means of different forms of crowdfunding.

Actors

There are basically three actors involved in the crowdfunding process itself: Capital recipients, capital donors and a platform. The capital recipients, who can be private individuals as well as organisations, are responsible, among other things, for promoting the project they are interested in, the implementation of which is actually up for financing. They publish their concerns, for example, in the form of a campaign on a platform on the Internet, on which the financing is specifically promoted or which, in the further course, also offers the forwarding to a payment service provider and informs about the progress of the campaign. Capital providers support the project advertised by the capital acceptors through their financial contributions, using the platform provided.

Models

Basically, a distinction is made between two forms of crowdfunding: crowdfunding with or crowdfunding without financial compensation.

One form of crowdfunding without financial consideration is donation-based crowdfunding. In this case, there is no (financial) compensation from the capital takers to the capital givers for the money raised. The purpose of a campaign is purely idealistic or charitable and the donors simply support the advertised 'good cause'. Likewise, reward-based crowdfunding or crowdfunding based on services in return does not require any monetary compensation. The incentive for the capital donors is, for example, a right of pre-emption on a certain innovative product before its official market launch.

Crowdfunding with financial consideration in the form of equity and borrowed capital-based crowdfunding, on the other hand, offers the capital providers concrete financial incentives in the form of monetary consideration for the contribution provided by them. For example, provided loans are repaid under a fixed agreed interest rate (crowd lending) or the capital providers receive a guaranteed profit share or company shares for their financial input (crowd investing).

53 Cf. https://www.bafin.de/DE/Aufsicht/FinTech/Crowdfunding/crowdfunding_node.html (accessed 20.08.2020).

National Cooperation

Cooperation with Law Enforcement Agencies

Cooperation with Supervisory Authorities

Requests from Domestic Authorities

Cooperation with the Reporting Entities under AMLA

National Cooperation

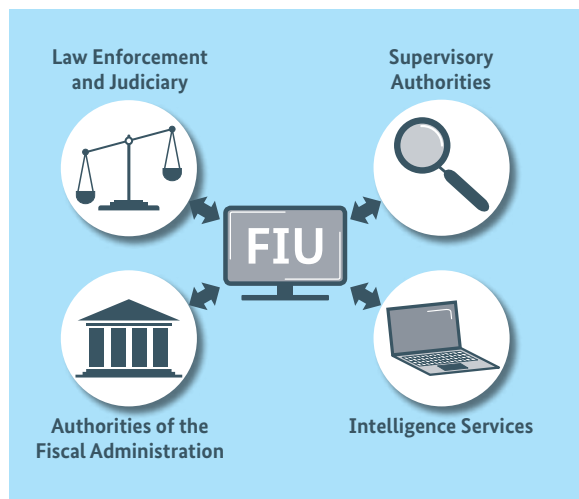


Figure 33: National Partner Authorities in the Overview

Intensive and sustained cooperation between the FIU and all national authorities within the network established by the provisions of the Anti-Money Laundering Act and other specialised laws is indispensable for the effective prevention of money laundering and terrorist financing. Particularly in view of the increasing complexity of economic subjects and the associated development of new technologies, continuous cooperation is strived for and constantly expanded. The FIU's national partner authorities include:

- the authorities of the fiscal administration (Federal Central Tax Office (BZSt), fiscal authorities of the Länder), as well as
 - the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND) and the Military Counter-Intelligence Service (MAD).
- For the collection and analysis of information in connection with money laundering and terrorist financing, in addition to cooperation with the national authorities, an active exchange with the reporting entities pursuant to Section 2 (1) AMLA is indispensable.

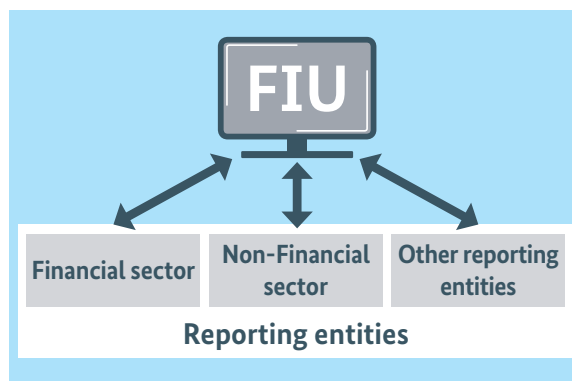


Figure 34: Reporting Entities

Due to the proliferation of Covid-19, the cooperation with national partner authorities and the reporting entities under the AMLA was faced with special challenges. Thus, due to the required restriction of contact, the exchange could not be continued as accustomed over previous years. The FIU therefore primarily intensified bilateral exchanges and – as far as possible – cooperation using modern means of communication.

Cooperation with Law Enforcement Agencies

Due to the pandemic, exchanges with national LEA could not take place in 2020 as in previous years. Classic forms of cooperation such as workshops, meetings and training sessions could only take place to a very limited extent, with a few virtual exceptions. Exceptions were bilateral talks at governance level as well as talks with the LKAs within the framework of the signing of administrative agreements on the occasion of the establishment of liaison officers of the FIU (FIU-LOs).

The biannual meeting with the LEA, specifically with the BKA, the LKAs, representatives of the financial investigations of the Länder, representatives of the public prosecution authorities (StA) of the Länder North Rhine-Westphalia and

Schleswig-Holstein as well as the Central Office for Organised Crime and Corruption Celle, could not take place in 2020 due to the pandemic situation. In order to further intensify cooperation and promote mutual understanding, the various topics of these events were discussed in telephone and video conferences. In this way, information was provided on the status of the IT projects, the management plan of the LEA, which is to be updated annually, as well as the reorientation of the FIU on the basis of the defined key risk areas and the associated priority handling of risk-relevant STRs. Due to the willingness of all partner authorities to cooperate, it was possible, despite the adverse circumstances, to have an ongoing, goal-oriented exchange.

Work Shadowing

The implementation of mutual work shadowing not only makes it possible to get to know the partner's working methods, but also enables direct professional exchange between the LEA and the FIU. Work shadowing is therefore a valuable component of cooperation.

In the reporting year, work shadowing could only be continued to a limited extent. The last two work shadowing visits by FIU employees at LEA took place in January 2020 at the LKAs Schleswig-Holstein. Due to the Covid-19 pandemic, all further work shadowing of FIU employees planned for 2020 has been postponed until further notice.

As they are mutually met with great interest and bring added value for all involved parties, they will be rescheduled for as soon as the pandemic situation allows.

For the year 2020, it was originally planned to include work shadowing by employees of the judiciary, the public prosecution authority in Frankfurt am Main and the Attorney General in Hamm. These, too, had to be postponed until further notice due to the Covid-19 pandemic.

Liaison Officers

The liaison officers of the FIU (FIU LOs) are the first direct contact persons of the FIU for questions regarding operational cooperation for the respective LEA (police, customs, tax investigation authorities, public prosecution authorities) as well as other cooperation partners of the FIU in the federal states. In addition, they accompany further process optimisations in the cooperation, especially with the police authorities and the public prosecution authorities. In terms of quality optimisation, they also ensure targeted communication of situation-relevant findings and can support the risk-based approach in the identification of key risk areas within the FIU.

With the piloting of the secondment in 2019, the secondment of the FIU LOs proved to be an effective means of promoting a direct and trusting exchange of information between LKAs and the FIU. As of the second quarter of the reporting year, the FIU LOs selected through an internal tendering process were therefore installed in almost all Länder as contact persons for the LEA as well as other stakeholders, such as the supervisory authorities of the non-financial sector.

As of December 2020, FIU LOs are now deployed in the LKAs in 15 Länder. As a rule, the FIU LOs are based in one LKAs, but – depending on the administrative agreement concluded – they are sometimes responsible for several Länder and are therefore also temporarily present at the respective other locations/ LKAs. As an example, the FIU LO at the LKA Schleswig-Holstein (headquarters) can be mentioned here. He is the contact person for all FIU cooperation authorities in Hamburg, Mecklenburg-Western Pomerania and Schleswig-Holstein.

This year, the FIU LOs were only able to participate in a few events due to Covid-19. Exceptions were inaugural visits to individual public prosecution authorities, tax investigation authorities and supervisory authorities of the financial and non-financial sector. The establishment of the FIU LOs in the respective Länder was generally very much welcomed by the partner authorities visited.

As of 31 December 2020, the FIU LOs had processed approximately 1,360 requests and other enquiries within the scope of operational cooperation with the LEA, thus significantly intensifying cooperation with the partner authorities.

Cooperation with Supervisory Authorities

Effective prevention and combating of money laundering and terrorist financing requires close cooperation between all authorities involved. In this respect, an intensive exchange of information between the FIU and the competent supervisory authorities of the financial and non-financial sectors is also indispensable.

Following the joint 'First Concerted Campaign against Money Laundering in the Automotive Sector', which was carried out for the first time in 2019, inter-agency cooperation between the FIU and the supervisory authorities of the Länder in the non-financial sector also took place in 2020. In this context, the FIU forwarded cases related to the risk focus of games of chance/betting to the competent supervisory authorities. Within the framework of the 'Concerted Campaign', the FIU actively supports the supervisory authorities in carrying out their risk-oriented tasks. At the same time, such actions raise awareness of money laundering prevention among the various reporting entities in the non-financial sector.

At the end of 2020, the FIU began transmitting information related to the art and antiques trade to the respective competent supervisory authorities. This information, which originates from STR, contains facts that trigger due diligence obligations for reporting entities and are thus relevant for the risk-oriented direction of supervisory examination measures. This action, which will be continued in 2021, also serves to raise awareness in the art sector, especially in light of the fact that the art sector was affected by new legal regulations in the reporting year. This includes, among other things, the expansion of the circle of reporting entities to include art warehouse keepers. In addition, the value limits that trigger due diligence obligations were decoupled from the method of payment. Thus, reporting entities in the art sector have to

fulfil due diligence obligations for transactions with a value of at least EUR 10,000, regardless of whether they are, for example, cash payments or bank transfers. With the targeted transmission of information from this sector, the FIU thus offers supervisory authorities an opportunity to sensitise the partly new reporting entities of the art sector by including concrete facts and to actively support them in the implementation of their obligations under money laundering law.

The close cooperation between the FIU and BaFin, as the supervisory authority for the financial sector, has always been characterised by various continuous as well as individual case-related meetings and is regularly expanded. A continuous exchange takes place, for example, with regard to the NRA. Individual case-related discussions relate, among other things, to questions from the group of reporting entities or money laundering risks with regard to certain types of accounts. In 2020, the 'Anti-Money Laundering Expert Group' was also established, which is a joint working group of the FIU and BaFin on operational issues and meets every two weeks. Here, concrete issues such as the assessment of the reporting quality of reporting entities are reviewed and common approaches are discussed.

The exchange of information and coordination with the domestic supervisory authorities could only take place to a limited extent in 2020 due to the Covid-19 pandemic. In February 2020, the FIU participated as a guest in an event of the supervisory authorities of the individual Länder in the games of chance sector in Fulda. Various topics and issues related to money laundering supervision and prevention were discussed there. It is intended to catch up on the already planned meetings and work shadowing agreements as soon as the situation allows.

Requests from Domestic Authorities

Through its extensive STR monitoring, the FIU has established itself as a firm partner in active support for criminal prosecution. The existing requests mostly include requests about suspects in a preliminary investigation. The transmission of personal data makes a valuable contribution to supporting the requesting authorities in their existing investigative procedures.

In this reporting year, the domestic authorities again made increased use of the possibility of national requests. Thus, the number of requests increased significantly once again. In particular, the number of requests from police authorities and the State Office of Criminal Investigation is a significant part of this.

In the year under review the total number of incoming national requests was 3,798 and thus increased by approximately 17% compared to the previous year. The number of national requests has thus increased for the third year in a row. The changes mainly result from an increased number of requests due to possible fraud offences in connection with Covid-19 emergency aid.⁵⁴

Request

By means of a request, domestic authorities, such as in particular LEA and intelligence services, may, under certain conditions, request personal data from the FIU, insofar as it appears necessary for the investigation of money laundering, terrorist financing or for the prevention of other dangers.

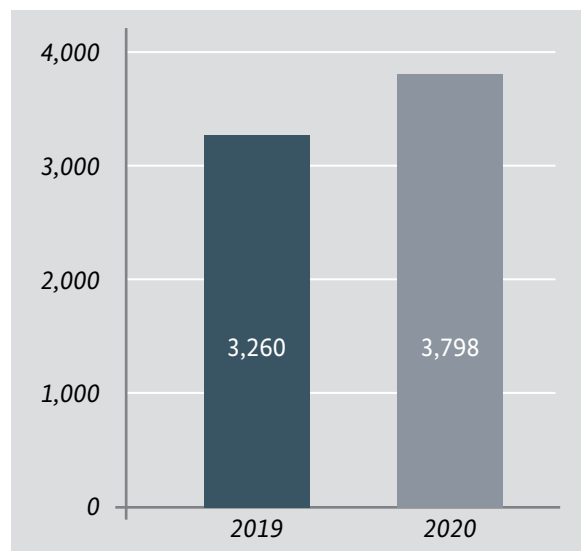


Figure 35: Incoming National Requests

⁵⁴ For more information on Covid-19 emergency aid fraud, see the comments 'Special topic Covid-19' in the section 'Typologies and Trends'.

The differentiation of national requests according to sender is as follows.

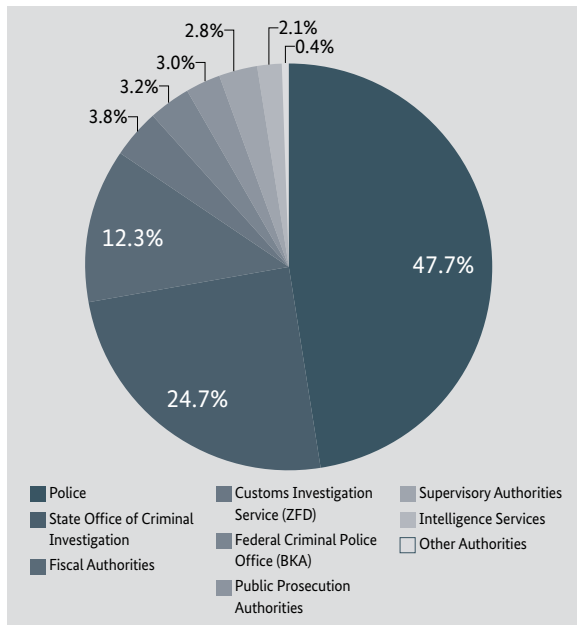


Figure 36: Breakdown of Domestic Requests by Sender

Compared to the previous year the LKAs as well as the fiscal authorities have sent more requests to the FIU. The supervisory authorities used frequently the means of submitting personal data requests to the FIU.

Case Study – Requests from Domestic Authorities⁵⁵

Within the framework of the 18th Parliamentary Investigation Committee of the Saxony-Anhalt State Parliament, the activities of so-called ‘big gamblers’ in the games of chance sector were investigated.

According to the findings of the gambling supervisory authority, a total of nine persons attracted attention in the case at hand due to high betting stakes, according to which betting stakes of approx. EUR 1.3 million were made and winnings of approx. EUR 1.5 million were achieved with a single customer card in 2018 alone (1). As a result, the FIU was requested by the relevant money laundering supervisory authority under Section 50 No. 8 AMLA (supervisory authority for organisers and brokers of games of chance) to submit existing information or STRs (2).

The FIU was able to establish various connections through existing STRs. A total of 22 STRs from banks and brokers and organisers of games of chance were already available in this context (3).

55 The case study presented is a real case from the FIU’s practice.

Furthermore, through the exchange with the FIU liaison officer in Saxony, it could be established that these persons are also already known there and that the police is investigating the matter (4).

The information contained in the report was processed by the FIU so that it could be disseminated to various LKAs (5).

Due to the good cooperation of the authorities and units involved and the FIU LOs, it was possible to prove extensive, supra-regional activities of the suspects involved. As a result, proceedings could be initiated and a lottery outlet licence could be revoked.

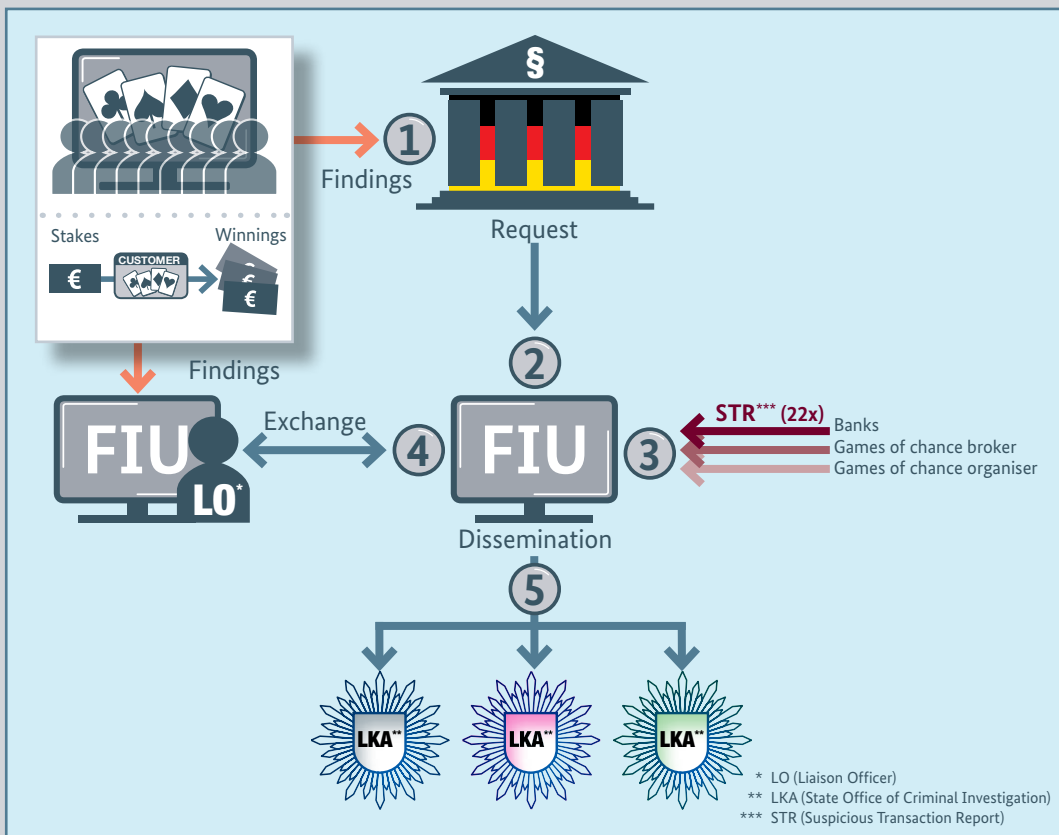


Figure 37: Case Study – Requests from Domestic Authorities

Numerous national requests received by the FIU in the reporting year were related to terrorist financing or state security-related crime. The FIU's specialised unit for terrorist financing exchanges information with the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND), the Military Counter-Intelligence Service (MAD), as well as the state security departments of the federal and state police authorities. The number of domestic requests related to terrorist financing or state security rose to a total of 343 in the reporting year, which corresponds to an increase of approximately 18%.

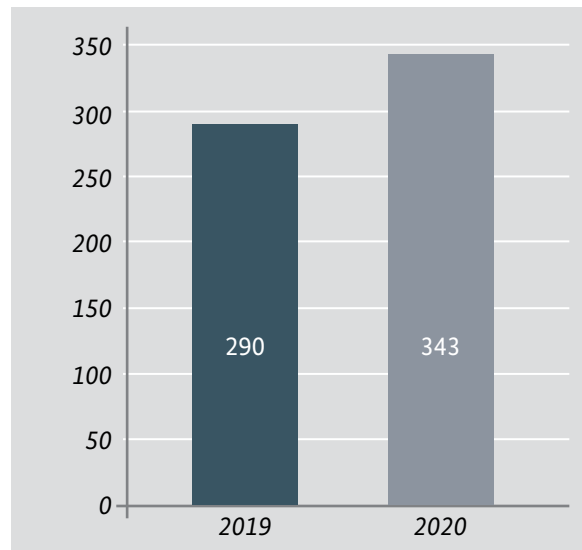


Figure 38: National Requests in the Area of Terrorist Financing and State Security

As in the previous year, almost half of the requests came from the LKAs. The second largest item in the reporting year was again the share of national requests received from intelligence services in the area of terrorist financing or state security with almost 22%. This is also the highest increase compared to the previous year (2019: 16.5%).

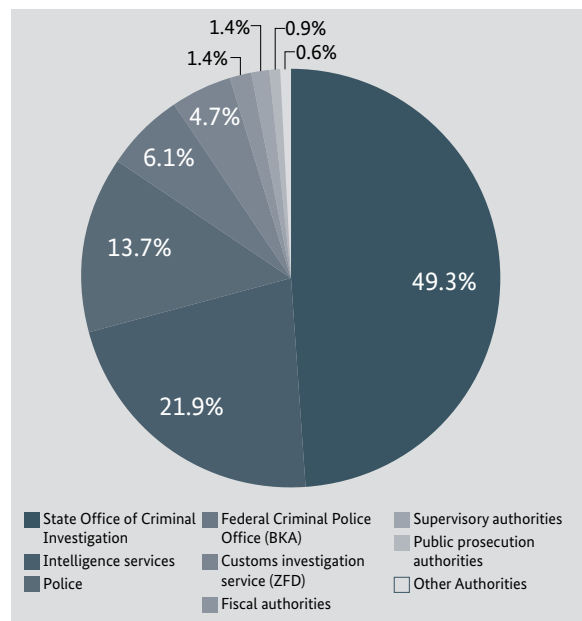


Figure 39: Breakdown of Domestic Requests in the Area of Terrorist Financing or State Security by Sender

Cooperation with Reporting Entities under AMLA

The previously successfully established forms of cooperation with reporting entities – in particular the money laundering conferences regularly organised by the FIU for representatives of the financial and non-financial sectors – could not take place in 2020 due to the pandemic. Nevertheless, continuous communication with reporting entities and associations was ensured through the increased use of digital channels. Extensive telephone conferences were held with individual reporting entities and groups of reporting entities in order to intensify the exchange and to compensate for unrealisable on-site appointments with reporting entities and the cancellation of five planned trade fairs. Numerous individual enquiries on various topics were increasingly answered by telephone and solutions to problems, especially technical problems, were offered.

External and also virtually organised events were accompanied by the FIU with specialist lectures. In particular, the FIU's operational key risk areas, combating money laundering under pandemic conditions and the FIU's international cooperation were discussed. In addition, attention was drawn to the new form of cooperation within the Anti Financial Crime Alliance (AFCA).⁵⁶

The FIU website was also regularly used as a central information portal to continuously provide current reports and technical information on the

reporting and registration procedure, among other things. Already at the beginning of the pandemic, findings of national and international partners as well as the FIU's own evaluations were published in a detailed warning on fraud and money laundering activities in connection with Covid-19. The aim was, on the one hand, to develop warnings for the citizens and, on the other hand, to sensitise the reporting parties in particular in the still early stage of the pandemic.

In the reporting year, a total of five new typology papers were published by the FIU:

- 'Special indications for insurance intermediaries',
- 'Fraud and money laundering activities related to Covid-19',
- 'Special indications for money laundering in the context of the collection of third-party or assigned receivables',
- 'Special indications in connection with watch and jewellery trade' and
- 'Special indications in connection with transactions involving virtual assets and virtual crypto business'.

⁵⁶ For more information on the AFCA, see the discussion on 'Public Private Partnership – Anti Financial Crime Alliance' later in this section.

The papers contain information on typical behaviour and conspicuous features in connection with money laundering and terrorist financing and thus make it easier for the reporting entities to recognise possible criminal acts or methods. The provision of two fact sheets with general requirements for the presentation of the facts when submitting a STR should also be emphasised in order to further facilitate cooperation with the obligated parties in the financial and non-financial sectors.

Feedback Reports

Pursuant to Section 41 (2) AMLA, reporting entities receive feedback on the relevance of submitted STRs, in particular to optimise their own risk management. The feedback concept, which was already consulted with the reporting entities and associations in 2018 and implemented in the following years, provides for reporting back information to the reporting entities on their respective reporting behaviour so that they can critically examine their reporting behaviour and, if necessary, make adjustments to their internal processes to fulfil their due diligence obligations. The FIU's feedback concept is subject to continuous further development. As of 1 January 2020, the feedback report was adapted to the conditions of the risk-based approach (RBA)⁵⁷. In this respect,

As part of the further expansion of the FIU, a separate area for the registration of reporting entities was created. Particularly with regard to the mandatory registration anchored in the AMLA (by 1 January 2024 at the latest), reporting entities in the financial and non-financial sectors have access to a competent team for questions and problems relating to registration and user management in goAML.

the feedback reports on STRs assessed by the FIU as of this date represent the next expansion stage of the feedback concept consulted in 2018. It now only includes reports on STRs that were assigned to the risk areas defined by the FIU for 2020.

Furthermore, the reporting intervals were set uniformly at quarterly intervals for 2020, regardless of the reporting intensity of the respective reporting entity. Thus, all reporting entities will receive an unsolicited quarterly report if they have submitted STRs that were assigned to a key risk area defined by the FIU for the year 2020 and were assessed accordingly with regard to their risk content. All other reporting entities will receive feedback on their STRs in a suitable form at least once a year.

⁵⁷ Against the background of the strengthening of the risk-based approach anchored nationally in the Anti-Money Laundering Act as well as in the EU Money Laundering Directive, taking into account the results of the NRA and in particular also the corresponding FATF requirements, the FIU has consistently continued the risk-oriented direction of its processes in accordance with the overall strategy of the Federal Government.

Public Private Partnership – Anti Financial Crime Alliance

In September 2019, a Public Private Partnership (PPP) between the authorities involved in preventing and combating money laundering and terrorist financing and the private sector was founded under the umbrella of the FIU. The 'Anti Financial Crime Alliance' (AFCA) was able to successfully expand and build up its strategic cooperation to combat money laundering and terrorist financing in 2020, initially for a period of three years. The structure of the AFCA continues to follow a partnership approach with equal input from all participants and thus provides the opportunity for a strategic, problem- and phenomenon-related exchange between government institutions and the private sector.

With the admission of 18 institutions, the AFCA now has a total of 36 members. It is particularly noteworthy that in the year under review, obligated parties and supervisory authorities from the non-financial sector also joined for the first time. Despite the Covid-19 pandemic, there was a regular, constructive and trusting exchange within the entire partnership as well as in individual working bodies (Board, Management Office and working groups).

In addition to the working groups '1 – Principles of Cooperation' and '2 – Risks and Trends in the Area of Money Laundering and Terrorist Financing in the Financial Sector', which were already established when the AFCA was founded, three further working groups began their activities in 2020. The focus here is on the topics '3 – Money Laundering in the Real Estate Sector', '4 – Tax Offences' and '5 – Games of Chance'. The participants of all working groups actively contribute to making the results as precise as possible with their professional expertise from their original activities within the respective sector. For example, the working group '3 – Money Laundering in the Real Estate Sector' includes representatives of the supervisory authorities, real estate agents, notaries, prosecutors and employees of credit institutions.

At the end of 2020, the team of experts was established and staffed with high-ranking representatives from the public and private sectors as well as an expert from academia. The team of experts will begin its work in 2021. In particular, it will support the Board with regard to the strategic objectives of the AFCA and analyse and evaluate the results of the working groups.

Membership structure of the AFCA (reporting period)	
Reporting Entities of the Financial Sector	19
Reporting Entities of the Non-financial Sector	7
Representatives of Authorities	8
Non-Reporting Entities ⁵⁸	2

⁵⁸ These are third parties who provide services for reporting entities without themselves being reporting entities under Section 2 (1) AMLA, such as the Federal Chamber of Notaries.

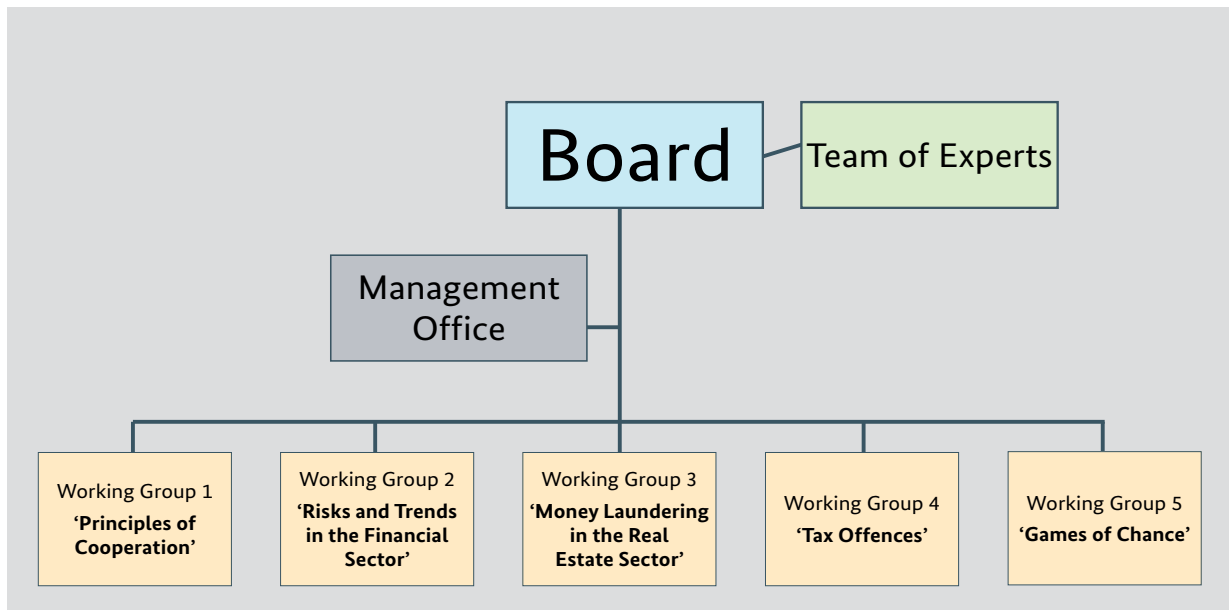


Figure 40: Structure of the AFCA

Two white papers were published by AFCA during 2020 ('Covid-19-related ML/CTF risks and implications for financial crime' and 'Covid-19-related ML/CTF risks and implications for financial crime 2.0'). The AFCA Forum 2020, which was held as an online conference in November 2020 due to the pandemic, was attended by over 100 representatives of reporting parties, authorities and international partners. In particular, a first positive assessment was made of the cooperation within AFCA since its foundation in September 2019. In addition, the working groups presented their main goals for 2021 and gave an outlook on the expected

results. These include a manual for recognising typologies for transaction and customer monitoring as well as the development of a transaction-related combined indicator model that makes it possible to filter out money laundering STRs in certain key risk areas and to share related information within the scope of what is legally permissible.

Only one year after its establishment, the AFCA has already proven to be a valuable instrument for cooperation between private sector institutions and the public sector.

International Cooperation

Information Exchange with other FIUs

International Committee Work

International Cooperation

The effective prevention and combating of money laundering and terrorist financing as cross-border and internationally occurring phenomena requires not only cooperation between national authorities but also collaboration with international

partners. The FIU Germany maintains an extensive exchange of information with other FIUs worldwide and is consistently involved in international committees and project work.

Information Exchange with other FIUs

The cooperation of the foreign FIUs within the Egmont Group⁵⁹ and the established communication channels are characterised by a high degree of efficiency and effectiveness and represent an essential element in the prevention and combating of internationally organised money laundering. Relevant information is continuously and proactively passed on or made available upon request.

Cooperation takes place on both the operational and strategic levels.

In the reporting year, the FIU exchanged information with a total of 145 countries. Cooperation with EU member states such as France, Luxembourg, Malta and Italy, as well as Great Britain⁶⁰, Switzerland and Russia was particularly close.

Incoming and Outgoing Information and Requests

The processing and analysis of international operational cases consolidated at a high level in 2020. Although the total number of cases of 9,270 is below the number of 11,865 achieved in the previous year, the number of requests increased to 2,842 cases (2019: 2,327), while the number of cases on spontaneous information decreased to 6,428 (2019: 9,538). Even under the pandemic-related restrictions, the FIU continued to successfully pursue its

international work to prevent and combat money laundering and terrorist financing.

Spontaneous Information

A spontaneous information is the proactive transmission of a fact that could be of importance to a partner FIU without being linked to a request sent by the partner authority.

⁵⁹ The Egmont Group is an international association of currently 166 FIUs worldwide. Its aim is the secure exchange of expertise and financial information to prevent and combat money laundering and terrorist financing.

⁶⁰ Great Britain left the European Union on 31 January 2021.

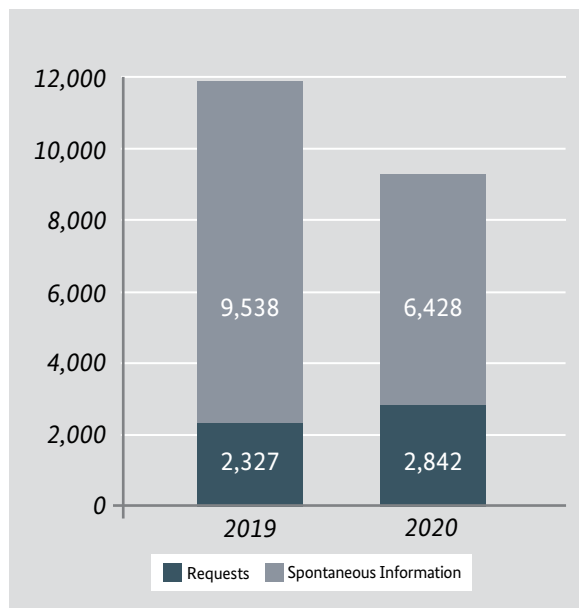


Figure 41: Cases of International Cooperation in Comparison to the Previous Year

For both spontaneous information and requests, a distinction is made between incoming and outgoing cases. The number of incoming requests in the reporting year was 1,250 (2019: 1,109) and has once again increased slightly compared to the previous year. The proportions of requests from EU and non-EU states have not shifted significantly and are within the range of usual fluctuation. The incoming requests are divided into 974 requests from EU countries and 276 requests from non-EU countries.

The incidents of incoming spontaneous information has once again increased significantly compared to the previous year to currently 1,451 (2019: 804). EU FIUs account for the majority of incoming cases regarding international cooperation (around 83%), with the FIUs in Malta and Luxembourg being particularly noteworthy. The FIU in Malta alone sent 529 spontaneous informations. A large number of these spontaneous information from the FIU Malta concern matters in connection with gambling and betting.

The trend also continues for outgoing international requests. Compared to the previous year, the total number of cases increased from 1,218 in 2019 to 1,592 in the reporting year. In contrast, incidents of outgoing spontaneous information decreased to 4,977 cases compared to 8,734 cases in 2019. The reason for this can be seen in the adjusted working methodology of FIU Germany taking into account the RBA. On the basis of the RBA, the FIU concentrates its filter function on those facts that are relevant for a foreign FIU based on the results of the analysis. At the same time, the spontaneous information sent has become both more comprehensive and more valuable.

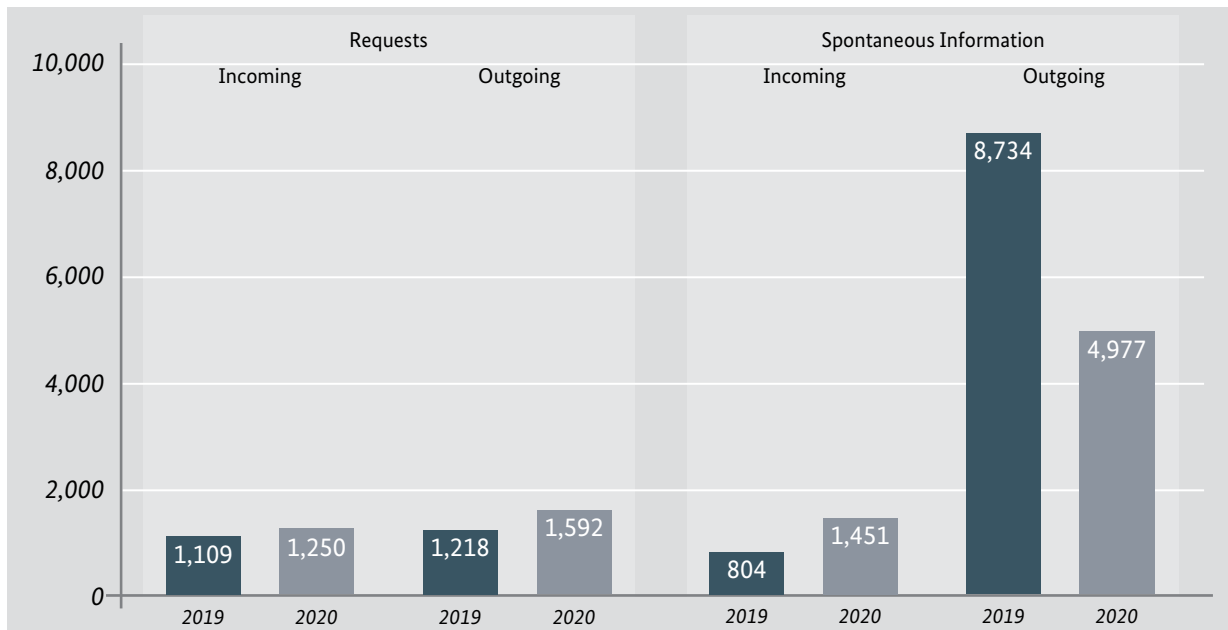


Figure 42: Requests and Spontaneous Information Compared to the Previous Year

In the reporting year, the FIU Germany received a total of 2,701 cases from almost 100 different FIUs worldwide. The following world map shows that by far the most cases of international cooperation (requests and spontaneous information) were submitted to the FIU Germany by Malta and Luxembourg, whereby these were mainly spontaneous

information. France also played an important role. The focus lay on requests. When it comes to FIUs from non-EU countries, there was an intensive exchange with Liechtenstein, Great Britain and Switzerland as well as with the USA and Russia.

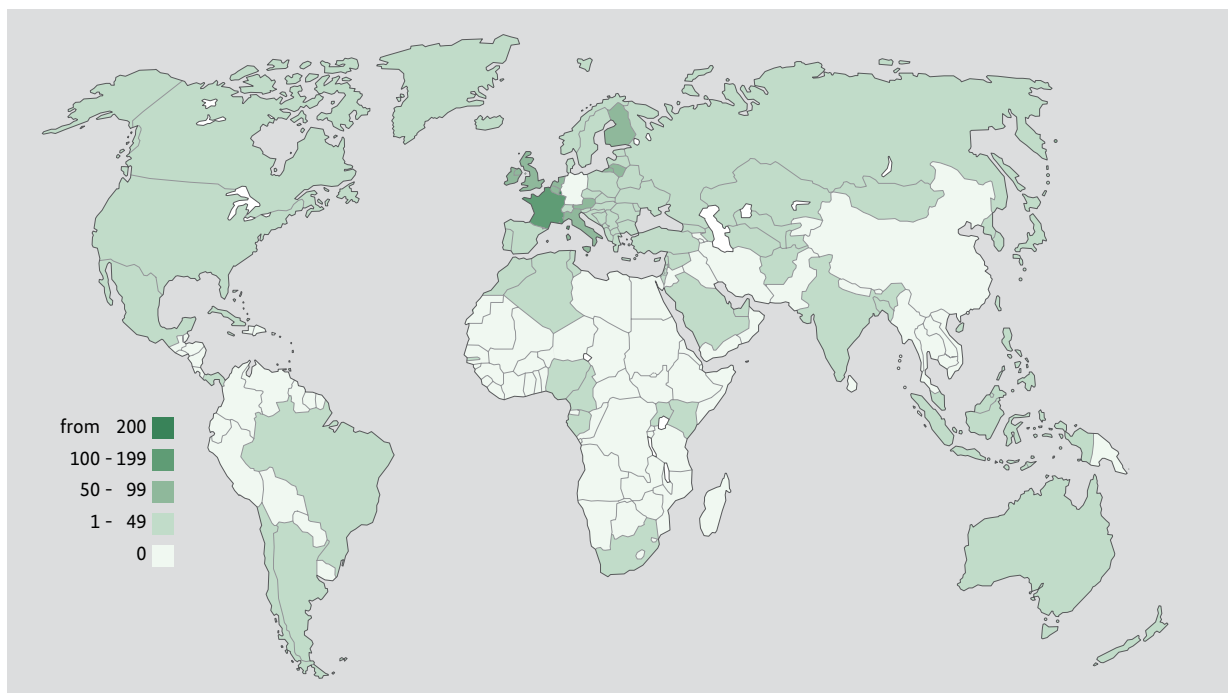


Figure 43: Incoming Cases of International Cooperation by Country of Origin

In the reporting year, the FIU Germany sent a total of 6,569 cases of international cooperation to more than 140 countries. Cooperation with France was particularly intense. In addition to the EU countries Italy, Poland, Spain, the Netherlands and

Luxembourg, the non-EU countries Great Britain, Switzerland, Russia, Turkey and the British Virgin Islands were frequent recipients of cases originating from Germany.

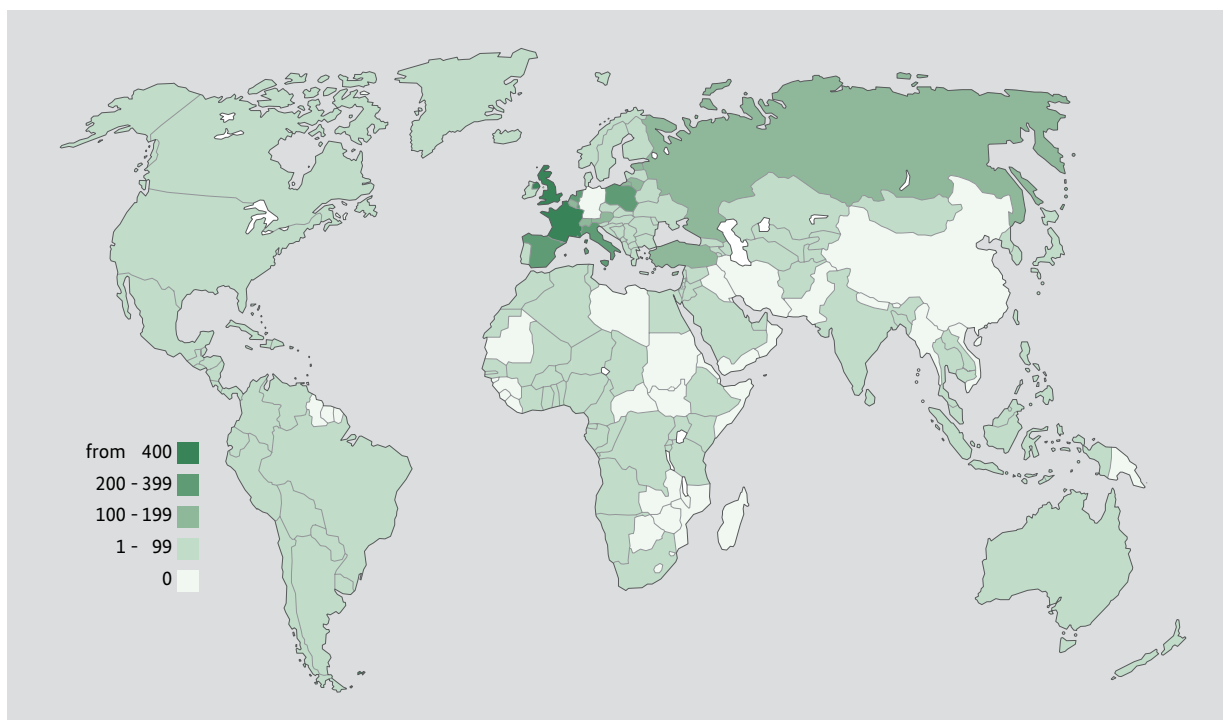


Figure 44: Outgoing Cases of International Cooperation by Country of Destination

The following tables provide an overview of the most important addressees and senders of incoming and outgoing requests and spontaneous information in the reporting year, measured in terms of the total number. As in 2019, the EU states France, Luxembourg and The Netherlands are the main recipients. Compared to the previous year, the

exchange of information with Poland plays a significantly greater role. Both in terms of outgoing requests and outgoing spontaneous information, it is in fourth place in 2020, with the number of outgoing requests almost doubling compared to the previous year.

Country	Incoming International Requests
France	170
Luxembourg	136
The Netherlands	69
Finland	61
Italy	59
Lithuania	54
Austria	42
Malta	42
Poland	39
Belgium	38
Other FIUs	538
Total	1,250

Country	Outgoing International Requests
Luxembourg	191
Great Britain	156
Spain	103
Poland	81
The Netherlands	76
Lithuania	66
Malta	59
Switzerland	56
Austria	54
Italy	49
Other FIUs	701
Total	1,592

Table 4: Number of Incoming and Outgoing Requests by Country

Country	Incoming Spontaneous Information
Malta	529
Luxembourg	346
Ireland	83
Liechtenstein	58
Belgium	52
Great Britain	50
Austria	38
Italy	31
Gibraltar	24
Hungary	21
Other FIUs	219
Total	1,451

Country	Outgoing Spontaneous Information
France	1,359
Italy	301
Great Britain	275
Poland	187
Cyprus	169
The Netherlands	160
Spain	143
Switzerland	132
Belgium	128
Austria	123
Other FIUs	2,000
Total	4,977

Table 5: Number of Incoming and Outgoing Spontaneous Information by Country

Case Study – International Requests in connection with Covid-19 Fraud Cases⁶¹

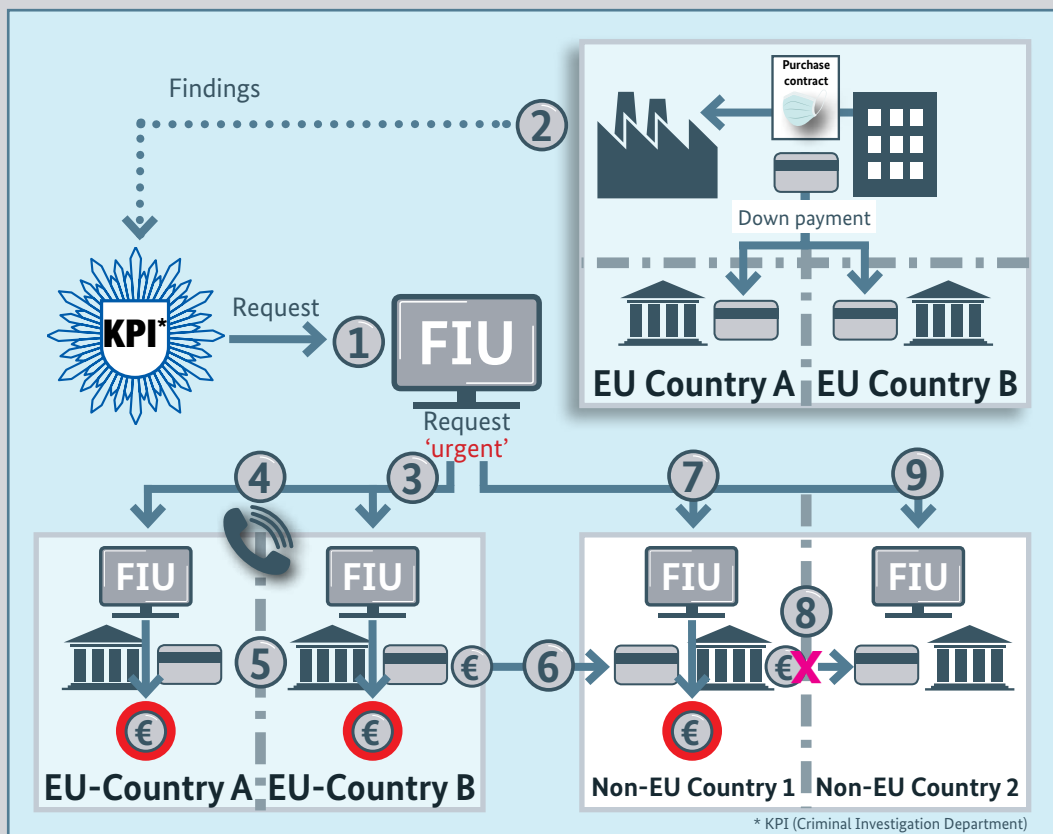


Figure 45: Case Study – International Requests in connection with Covid-19 Fraud Cases

The FIU received a request from a domestic criminal investigation department (KPI) (1). The aim was to initiate seizure measures concerning target accounts in two European countries. The background was a case of fraud in connection with the sale of protective masks. Through a sales company, 10 million protective masks were ordered and a deposit of EUR 14.7 million was transferred to accounts in EU country A and EU country B (2). The sales company used a business contact to approach a company based in another EU country that should arrange the deal through two distributors based in Europe. The protective masks were to be transferred to a storage location in country B. For this purpose, 52 trucks were made available via the sales company. An employee of the sales company and an employee of the intermediary were at the agreed time at the supposed place of delivery. However, the delivery did not take place. As a result, a complaint was filed in country B and later in Germany. Requests were made to the FIU in EU country A and to the FIU in EU country B (3).

61 The case study presented is a real case from the FIU's practice.

The requests were marked as 'urgent', and in parallel the colleagues of the FIUs were informed of the urgency by telephone (4). In the EU countries, seizure measures were initiated to freeze the funds transferred there. By this means, the sum transferred to EU country A could be completely seized, as well as a part of the sum in EU country B (5). However, the majority of the funds in EU country B had already been transferred to a non-EU country 1 (6). This was followed by another request, this time to non-EU country 1 (7). The seizing measures taken there led to the freezing of the funds and prevented further transfers to another non-EU country 2 (8). Since the people behind the transfer were suspected to be there, another request was made (9).

Through quick, cross-border action and cooperation between the authorities, it was possible to successfully take seizing measures. The assets were almost completely recovered. A group of perpetrators was caught and taken into custody in EU country B. One of the people behind the fraud was also found in non-EU country 2. Additionally, it was also possible to identify one of the people behind the crime in non-EU country 2.

There is also an ongoing exchange of information at the international level in the area of terrorist financing and state security. In the reporting year, the FIU Germany received a total of 273 cases from 34 partner FIUs, which were divided equally between requests and spontaneous information.⁶² While the number of incoming spontaneous information was 136, roughly the same as the previous year (2019: 124), incoming requests increased sharply from 97 in 2019 to 137 in 2020. As in the previous year, cooperation with the FIU France was particularly intense. A strong increase was observed in the area of incoming requests from the FIU Luxembourg. The number of requests sent rose from 6 in the previous year to 33 in 2020. As in 2019, the majority of spontaneous information was sent by Luxembourg and the USA.

In 2020, the FIU Germany sent a total of 75 requests to 28 countries worldwide for the prevention of terrorist financing and other crimes relevant to the security of the state. While both the number of outgoing cases and their distribution among requests and spontaneous information remained roughly the same compared to the previous year, the number of countries to which the cases were sent increased. As in the previous year, cooperation with Luxembourg, Great Britain, Turkey and France was particularly profound.

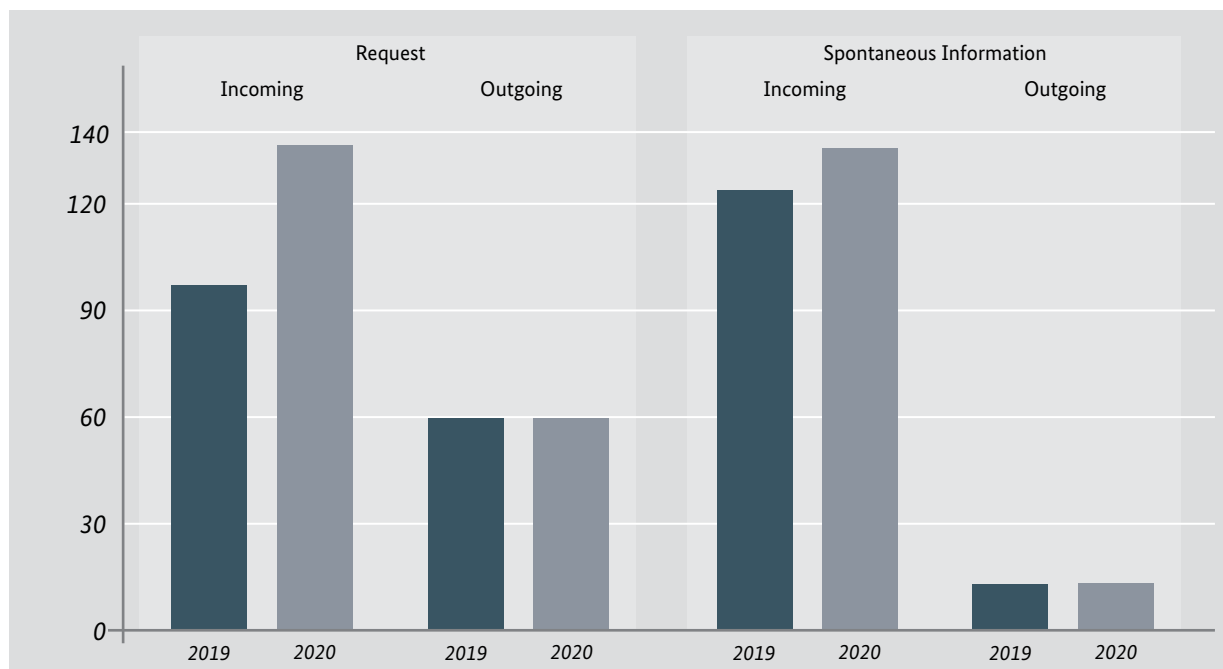


Figure 46: Cross-border Information Exchange Related to Terrorist Financing/State Security

62 This and the following figures on terrorist financing/state security related requests and information are a subset of the total figures on requests and information presented earlier in this chapter.

Country	Incoming requests
France	36
Luxembourg	33
Tajikistan	6
Belgium	6
USA	5
The Netherlands	5
Russia	4
Austria	4
Finland	4
Malta	4
other FIUs	30
Total	137

Country	Outgoing requests
Luxembourg	20
Great Britain	8
Turkey	6
The Netherlands	3
Sweden	3
other FIUs	21
Total	61

Country	Incoming Spontaneous Information
Luxembourg	111
USA	9
Belgium	2
Malta	2
Japan	2
other FIUs	10
Total	136

Country	Outgoing Spontaneous Information
France	4
Switzerland	2
Austria	2
Great Britain	2
other FIUs	4
Total	14

Table 6: Number of Incoming and Outgoing Spontaneous Information and Requests related to Terrorist Financing/State Security by Country

International Committee Work

The intensification and optimisation of its international relations enable the FIU to actively promote the improvement of the conditions for preventing and combating money laundering and terrorist financing, to pick up on new trends and challenges at an early stage and to develop solution strategies together with FIUs worldwide.

The results of the continuous expansion of international relations over the past years have become particularly evident in the unprecedented pandemic situation. The close exchange between the FIUs and other organisations involved, e.g. through virtual international workshops, made it possible to adapt quickly and efficiently to the changed conditions and to initiate proactive measures to combat new *modi operandi*.⁶³ In addition to the FATF publication 'Covid-19-Related Money Laundering and Terrorist Financing Risks' listed below, these were also discussed at virtual working group meetings of the Egmont Group. In addition, there were virtual workshops on the Egmont Group's ECOFEL learning platform.

With regard to other topics, the FIU also managed to continue its international committee work, despite difficult conditions, thanks to the possibility of digital networking. In the reporting year, the regular exchange among the German-speaking FIUs of Luxembourg, Liechtenstein, Austria and Switzerland was again ensured, this time also including the FIU Netherlands.

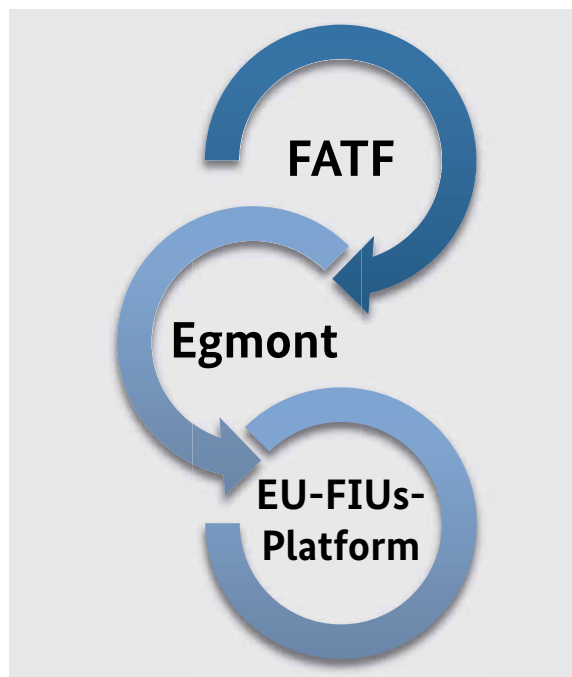


Figure 47: International Committees

The importance of international committee work is obvious, especially in this challenging year. The FIU will therefore continue to work on the reinforced expansion of international cooperation.

Furthermore, in addition to the exchange of operational knowledge in the area of requests, the FIU is in continuous professional exchange with foreign FIUs, e.g. on European and national legislative proposals or the implementation of EU directives.

⁶³ For the new *modi operandi* under the Covid-19 situation, see also 'Special Topic Covid-19' in the section 'Typologies and Trends'.

Financial Action Task Force (FATF)

As the most important international body for preventing and combating money laundering, terrorist and proliferation financing, the FATF sets globally valid standards, whose compliance and effective implementation is regularly reviewed.

The FATF was founded in 1989 by the G7 countries. Today, the FATF has 39 members, 37 member states, the EU Commission and the Gulf Cooperation Council. In addition, the FATF is the 'parent' institution of a network of nine regional partner organisations, so that more than 200 jurisdictions worldwide have committed themselves to implementing the FATF standards.

With the election of Ministerialdirigent (Head of Section) Dr Marcus Pleyer as the first two-year FATF President in July 2020, Germany is prominently represented in the FATF.

The FIU is part of the German FATF delegation under the leadership of the Federal Ministry of Finance (BMF) and actively contributes to the various FATF projects. In 2020, the FIU was intensely involved in the FATF publication 'Covid-19-Related Money Laundering and Terrorist Financing Risks' and, as project lead of an Egmont Group project, provided considerable contributions to the TBML-report 'FATF/Egmont Trade-based Money Laundering: Trends and Developments'⁶⁴. The FIU also contributes its expertise to the priority topics of the German FATF Presidency, such as the ongoing project 'Financing of Ethnically or Racially Motivated Terrorism'.

⁶⁴ See the following explanations in the course of this section.

Egmont Group of FIUs

The Egmont Group ('Egmont Group of FIUs') is a global association of FIUs that provides a platform for the secure exchange of expertise and financial information to combat money laundering and terrorist financing. It now comprises 166 members worldwide.

The pandemic-related restrictions were also a major challenge for the Egmont Group. Nevertheless, the FIU succeeded in further expanding its international role. The FIU was able to contribute its technical expertise by continuing to successfully chair the 'Information Exchange Working Group' (IEWG), which is an important body for the entire Egmont Group, and by actively participating in the 'Membership, Support and Compliance Working Group' (MSCWG) and in the Europe I Regional Group. At its annual plenary meeting, which was held online this time due to the pandemic, the Egmont Group elected the deputy head of the FIU as vice-chair of the Egmont Group. By assuming this role, the FIU occupies a key position in the multinational network and thus once again demonstrates its commitment to international cooperation.

Noteworthy, in particular, are the significant highlights the FIU set through its work in the IEWG. With the projects listed below, the FIU has made a significant contribution to improving the worldwide prevention of and fight against money laundering and terrorist financing.

The products from the IEWG projects provide valuable insights not only for FIUs, but also for national authorities and reporting entities. Within Work

Stream III of the project 'Conclusions from large scale cross border Money Laundering schemes'⁶⁵, a 'Case Book' was compiled: It contains a collection of case studies relating money laundering in 'laundromats', collected by a number of different international FIUs participating in this project. Within the framework of the projects 'Combatting Online Child Sexual Abuse and Exploitation' and 'Money Laundering of the proceeds of serious tax crimes', for each project a confidential report was prepared for forwarding to LEA and reporting entities. In addition to that, public summaries were also published on the FIU website. The project 'Human Trafficking – Phase II' resulted in a collection of recommendations that support the FIUs in their fight against human trafficking

In addition to the aforementioned completed topics, the IEWG is dedicated to the following projects:

- 'Conclusions from large scale cross border Money Laundering schemes',
- 'Asset Recovery – the role of FIUs',
- 'E-Catalogue on Regulated Virtual Asset Service Providers (VASPs)',
- 'FIU's capabilities and involvement in the fight against the financing of extreme right-wing terrorism'.

65 See the following explanations in the course of this section.

International Cooperation Project**‘Conclusions from large scale cross border Money Laundering scheme’**

The uncovering of various money laundering scandals in recent years, including in particular the so-called ‘laundromats’, impressively revealed the immense scale of cross-border money laundering systems and networks: according to estimates by international research networks, over 20 billion USD passed through the so-called Russian Laundromat⁶⁶ between 2010 and 2014, between 2012 and 2014, about EUR 2.5 billion were washed via the so-called Azerbaijan Laundromat⁶⁷. In 2018, it became public that suspicious payments amounting to EUR 200 billion allegedly went through the Estonian branch of Danske Bank,⁶⁸ followed in 2019 by the uncovering of the ‘Troika Laundromat’.

But what happens after such ‘laundromats’ are shut down? What are the new avenues and routes that money launderers use to bring incriminated funds into the legitimate economic cycle?

To find some possible first answers to these questions, FIU Germany initiated an international strategic analysis project within the Egmont IEWG in July 2019. The project ‘Conclusions from large scale cross border money laundering schemes’ is led by FIU Germany, with the project team including eleven other FIUs as well as the FATF Risks, Trends and Methods Group (RTMG). The aim of this project is to derive insights and findings from the analysis of past cross-border money laundering schemes and to develop useful approaches to identify such schemes in the future. The project not only benefits from the collected data and experiences of the different FIUs involved, but also carries out joint strategic data analyses within the framework of the project.

The project consists of three work streams. Work Stream I and II focus on data collection and on the analysis of transactional data. Following a jointly defined approach, the project conducts, among other things, an empirical testing of risk indicators in order to possibly see how individual risk indicators perform within the sample and whether there are possible correlations between different indicators. This work was started in 2020 and will continue in 2021.

Work Stream III is dedicated to the collection of case studies, best practices and modus operandi from large scale cross-border money laundering schemes and was successfully completed at the end of 2020. In this work stream, the topic of TBML was identified as particularly relevant, therefore, the project put a dedicated focus on TBML-related schemes and techniques. Furthermore, insights and findings on TBML-related schemes and issues were also collected for input into the joint FATF and Egmont Group work on TBML and into the joint TBML-report⁶⁹.

The project contributes to an intensified and fruitful cooperation on international level. Valuable insights on large scale cross-border money laundering schemes are being pooled and shared, which not only strengthens international cooperation but also contributes to a common positioning in the fight against international money laundering.

66 Cf. Organized Crime and Corruption Reporting Project (OCCRP), <https://www.reportingproject.net/therussianlaundromat/>, accessed on 03.03.2021.

67 Cf. OCCRP, <https://www.occrp.org/en/azerbajjanilaundromat/>, accessed on 03.03.2021.

68 Cf. Bruun & Hjejle (2018), Report on the Non-Resident Portfolio at Danske Bank’s Estonian branch, <https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-estonian-branch.pdf?rev=56b16dfd4ae94480bb8cdcaebadddc9b&hash=B7D825F2639326A3BBBC7D524C5E341E>.

69 FATF – Egmont Group (2020), TBML: Trends and Developments, FATF, Paris, France, www.fatf-gafi.org/publications/methodandtrends/documents/trade-based-money-laundering-trends-and-developments.html.

EU FIUs Platform

In 2006, the European Commission established the EU FIU Platform with the aim of facilitating the exchange of information between European FIUs and promoting their cooperation.

In 2020, FIU Germany was once again able to make valuable contributions to the informal expert rounds that took place on a regular basis. We developed and contributed positions on preventing and combating money laundering and terrorist financing in close coordination with the EU FIUs. In this way, the FIU was able to set a clear course in the conceptual development of the European Coordination and Support Mechanism (CSM) at the EU level with its technical and coordinating participation. With a coordinating role of FIU Germany, a working group consisting of eleven other European FIUs has developed proposals for the function and structure of the Coordination and Support Mechanism. The implementation is

intended to significantly strengthen the work of the FIUs both at the operational and strategic level as well as in European cooperation, also with other stakeholders at the EU level.

In addition, the FIU was able to successfully contribute its expert knowledge to a joint project of various European FIUs on the operational analysis of TBML. The aim of the project was to analyse and evaluate various flows of goods and financial funds between Asia and Europe.

Another focus of the platform was the further development of FIU.net. The FIU.net system is one of the existing information channels for the secure exchange of data and information between the European FIUs. The necessary IT infrastructure will be provided by the European Commission in the future.

List of Figures

Figure	Title	Page
1	Process Sequence for Operational Analysis	14
2	Development of the Number of Suspicious Transaction Reports According to the AMLA (2010 – 2020)	15
3	Relative Proportion of Suspicious Transaction Reports Related to Potential Terrorist Financing or State Security	16
4	Increase of Reporting Entities Registered with the FIU	18
5	Registration Behaviour of Selected Subgroups of Reporting Entities	19
6	Breakdown of Reports by Recipients of Dissemination	23
7	Distribution of the Submitted Analysis Reports Among the Federal States	23
8	Number of Feedback Reports from Public Prosecution Authorities	24
9	Overview of Convictions, Penalty Orders, Decisions and Indictments	24
10	Case Study – Feedback Reports from Public Prosecution Authorities	26
11	Case Study – Temporary Freezing Order	29
12	Foreign Involvement in Suspicious Transactions	32
13	Number of Suspicious Transactions by Country of Origin	33
14	Number of Suspicious Transactions by Country of Destination	34
15	FIU Key Risk Areas	37
16	Received Suspicious Transaction Reports with reference to Covid-19	39
17	Case Study – Emergency Aid Fraud I	41
18	Case Study – Emergency Aid Fraud II	43
19	Case Study – Trade-based Money Laundering	45
20	Case Study – Protective Mask Sales	47
21	Case Study – Reich Citizen	50
22	Case study – Covid-19 Emergency Aid Fraud by Humanitarian Associations	51
23	Modus Operandi – Over-Invoicing of Goods	55
24	Modus Operandi – Third-Party Intermediaries Facilitating Invoice Settlement	56
25	Case Study – Commercial Fraud	58
26	Development of the Number of Case Analyses with reference to Key Risk Area Commercial Fraud (and Identity Theft)	59
27	Case Study – Identity Theft	61
28	Suspicious Transaction Reports with the Reporting Reason ‘Anomalies in Connection with Virtual Currencies’	64
29	Case study – Suspicious Account and Transaction Network	66
30	Case Study – Money Laundering of Fraudulently Obtained Covid-19 Emergency Aid	67
31	Further Reports in the Key Risk Area ‘Use of New Payment Methods’	68
32	Case Study – Network with Financial intermediaries	70
33	National Partner Authorities in the Overview	78
34	Reporting Entities	78
35	Incoming National Requests	82
36	Breakdown of Domestic Requests by Sender	83
37	Case Study – Requests from Domestic Authorities	84
38	National Requests in the Area of Terrorist Financing and State Security	85

Figure	Title	Page
39	Breakdown of Domestic Requests in the Area of Terrorist Financing or State Security by Sender	85
40	Structure of the AFCA	89
41	Cases of International Cooperation in Comparison to the Previous Year	93
42	Requests and Spontaneous Information Compared to the Previous Year	94
43	Incoming Cases of International Cooperation by Country of Origin	94
44	Outgoing Cases of International Cooperation by Country of Destination	95
45	Case Study – International Requests in Connection with Covid-19 Fraud Cases	97
46	Cross-border Information Exchange Related to Terrorist Financing/State Security	99
47	International Committees	101

List of Tables

Table	Title	Page
1	Number of Suspicious Transaction Reports According to Subgroups of Reporting Entities	17
2	Number of Active Reporting Entities	21
3	Proportion of Suspicious Transaction Reports submitted	22
4	Number of Incoming and Outgoing Requests by Country	96
5	Number of Incoming and Outgoing Spontaneous Information by Country	96
6	Number of Incoming and Outgoing Spontaneous Information and Requests related to Terrorist Financing/State Security by Country	100

List of Abbreviations

Abbreviation	Explanation
AFCA	Anti Financial Crime Alliance
AMLA	Anti-Money Laundering Act, act on tracing profits from serious criminal activities ('GwG Geldwäschegesetz') in the version dated 23 June 2017, as last amended by Article 6 (3) of this Act on 15 January 2021.
AO	German Tax Code ('Abgabenordnung'), valid in the version dated 1 October 2002, as last amended by Article 3 of this Act on 28 March 2021
BaFin	Federal Financial Supervisory Authority
BfV	Federal Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BMF	Federal Ministry of Finance
BND	Federal Intelligence Service
CSM	Coordination and Support Mechanism
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FIU LOs	FIU Liaison Officers
FKS	Financial Control of Illicit Employment
GZD	Central Customs Authority
IEWG	Information Exchange Working Group
ITZBund	Federal Information Technology Centre
KPI	Criminal Investigation Department
LEA	Law Enforcement Agencies
LKA/LKAs	State Office(s) of Criminal Investigation
MAD	Military Counter-Intelligence Service
MSCWG	Membership, Support and Compliance Working Group
NGO	Non-Governmental Organisation
NPO	Non-Profit Organisation
NRA	National Risk Assessment
PPP	Public Private Partnership
RBA	Risk-based approach
RTMG	FATF Risks, Trends and Methods Group
StA	Public Prosecution Authorities
StPO	Code of Criminal Procedure, in the version of 7 April 1987, last amended by Act of 30 March 2021 with effect from 2 April 2021
TBML	Trade Based Money Laundering

■ LEGAL NOTICE:

Published by:

Central Customs Authority
Financial Intelligence Unit (FIU)
P.O. Box 85 05 55
D-51030 Cologne

Edited by:

Central Customs Authority (GZD)

Design and creation:

Central Customs Authority (GZD), Training and Science Centre of the Federal Revenue Administration

Registration number:

90 SAB 272

www.zoll.de

Cologne, October 2021

www.fiu.bund.de